Scanning Networks

Module 03

Scanning a Target Network

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Earlier, you gathered all possible information about the target such as organization information (employee details, partner details, web links, etc.), network information (domains, sub-domains, IP addresses, network topology, etc.), and system information (OS details, user accounts, passwords, etc.).

Now, as an ethical hacker, or as a penetration tester (hereafter, pen tester), your next step will be to perform port scanning and network scanning on the IP addresses that you obtained in the information-gathering phase. This will help you to identify an entry point into the target network.

Scanning itself is not the actual intrusion, but an extended form of reconnaissance in which the ethical hacker and pen tester learns more about the target, including information about open ports and services, OSes, and any configuration lapses. The information gleaned from this reconnaissance helps you to select strategies for the attack on the target system or network.

This is one of the most important phases of intelligence gathering, which enables you to create a profile of the target organization. In the process of scanning, you attempt to gather information, including the specific IP addresses of the target system that can be accessed over the network (live hosts), open ports, and respective services running on the open ports and vulnerabilities in the live hosts.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Port scanning will help you identify open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is also used to discover the vulnerabilities in the services running on a port.

The labs in this module will give you real-time experience in gathering information about the target organization using various network scanning and port scanning techniques.

Lab Objectives

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

- Check live systems and open ports
- Identify services running in live systems
- Perform banner grabbing/OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Scanning Networks

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port Scanning**: Lists open ports and services
- **Network Scanning**: Lists the active hosts and IP addresses
- **Vulnerability Scanning**: Shows the presence of known weaknesses

Lab Tasks

Ethical hackers and pen testers use numerous tools and techniques to scan the target network. Recommended labs that will assist you in learning various network scanning techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Host Discovery	√	√	√
	1.1 Perform Host Discovery using Nmap	√		√
	1.2 Perform Host Discovery using Angry IP Scanner		√	√
2	Perform Port and Service Discovery	√	√	√
	2.1 Perform Port and Service Discovery using MegaPing		√	√

	2.2 Perform Port and Service Discovery using NetScanTools Pro		√	√
	2.3 Explore Various Network Scanning Techniques using Nmap	√		√
	2.4 Explore Various Network Scanning Techniques using Hping3		√	√
3	Perform OS Discovery	√	√	√
	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark		√	√
	3.2 Perform OS Discovery using Nmap Script Engine (NSE)	√		√
	3.3 Perform OS Discovery using Unicornscan		√	√
4	Scan beyond IDS and Firewall	√	√	√
	4.1 Scan beyond IDS/Firewall using various Evasion Techniques	√		√
	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall		√	√
	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall	√		√
	4.4 Create Custom Packets using Nmap to Scan beyond IDS/Firewall		√	√
	4.5 Browse Anonymously using Proxy Switcher		√	
	4.6 Browse Anonymously using CyberGhost VPN		√	
5	Draw Network Diagrams		√	√
	5.1 Draw Network Diagrams using Network Topology Mapper		√	√
6	Perform Network Scanning using Various Scanning Tools	√		√
	6.1 Scan a Target Network using Metasploit	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Perform Host Discovery

Host discovery is the process of identifying active hosts in the target network.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap
- Perform host discovery using Angry IP Scanner

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nmap located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**
- Angry IP Scanner located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
    - ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
    - TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol scan

Lab Tasks

TASK 1

Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. Turn on one or more virtual machines. In this lab task, we have used the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines.

2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

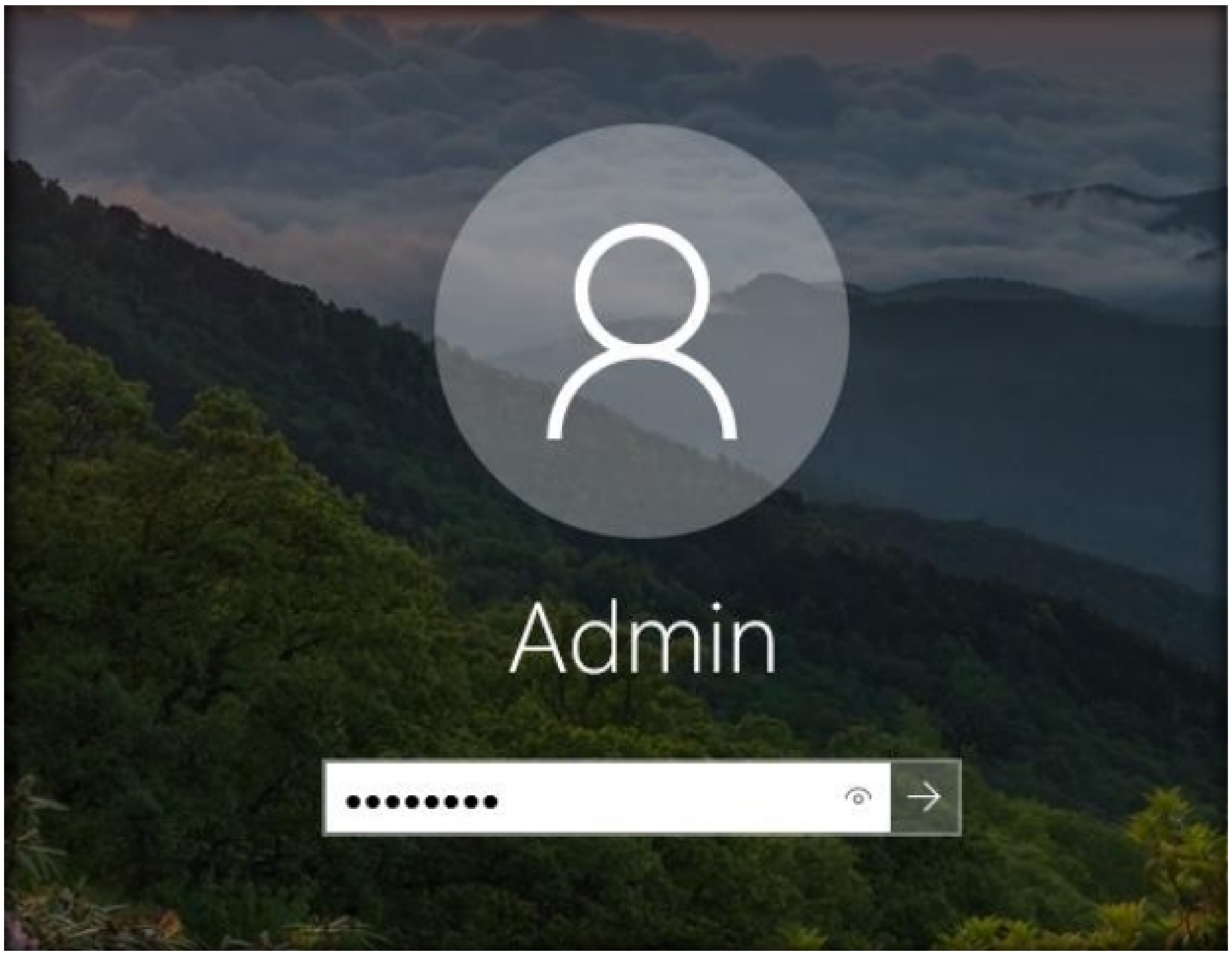


Figure 1.1.1: Login window

TASK 1.1

Install Nmap

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**; then, double-click **nmap-7.80-setup.exe**.

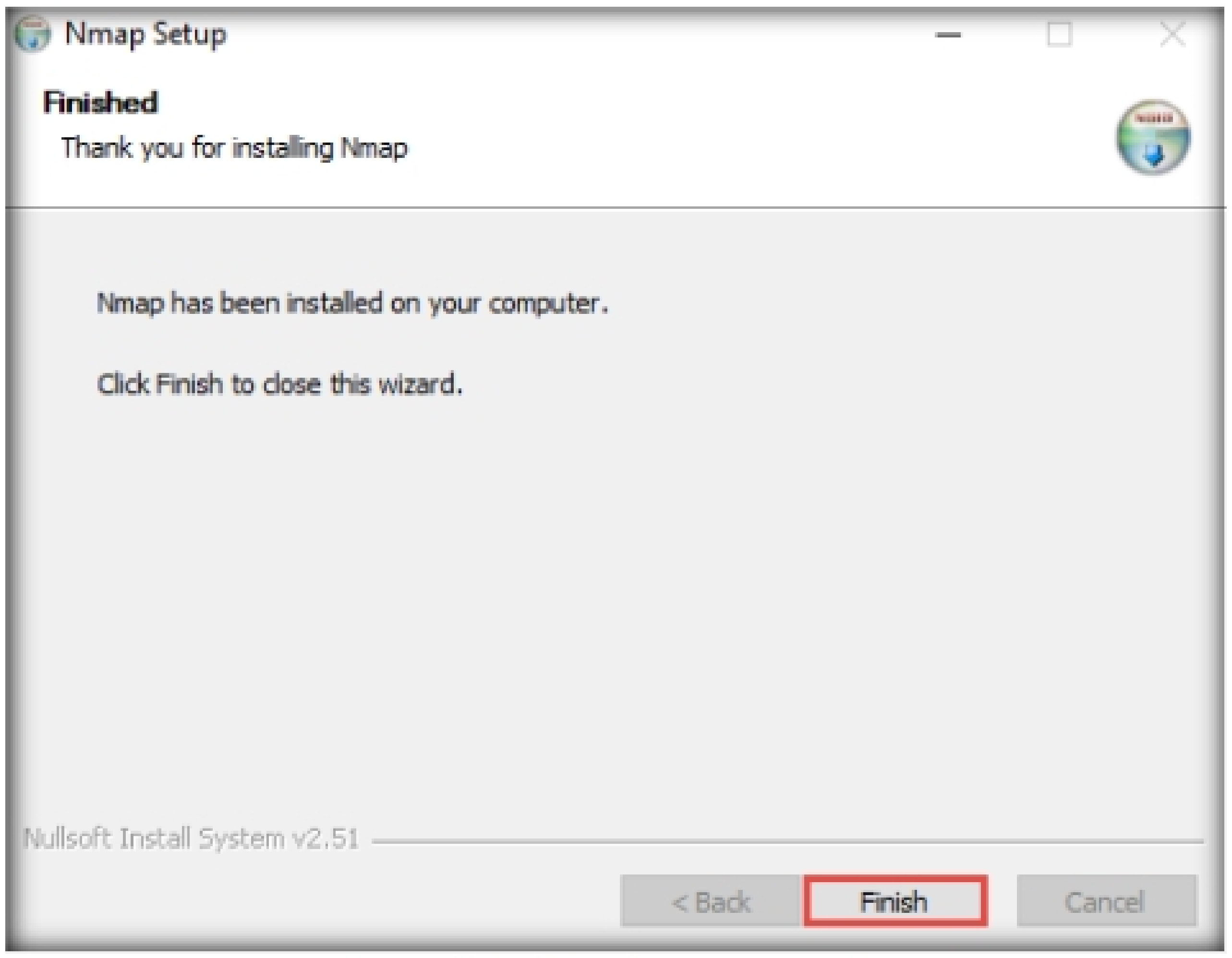
Note: If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. In the **Nmap Setup** window, click **I Agree** and follow the installation steps to install Nmap using all default settings.

Note: If an **Npcap Setup** window appears, click **Install** and follow the installation steps. After the completion of the installation, click **Finish**.

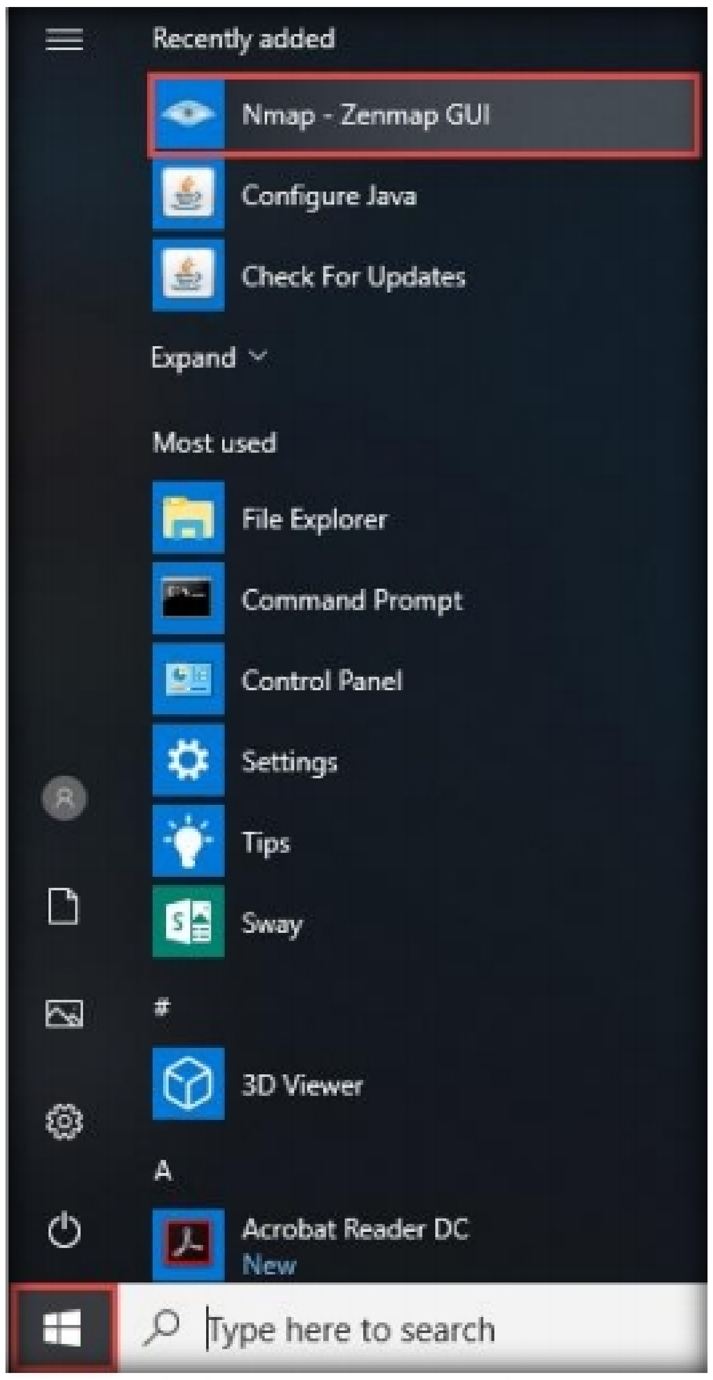
5. In the **Nmap Setup** window, follow the wizard-driven steps to install Nmap and click **Finish**.



Nmap Setup
Finished
Thank you for installing Nmap
Nmap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v2.51
< Back
Finish
Cancel

Figure 1.1.2: Nmap Setup pop-up wizard

6. On the completion of the installation, click on the **Start** menu on the bottom-left corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.



Recently added
Nmap - Zenmap GUI
Configure Java
Check For Updates
Expand
Most used
File Explorer
Command Prompt
Control Panel
Settings
Tips
Sway
#
3D Viewer
A
Acrobat Reader DC
New
Type here to search

Figure 1.1.3: Launch Nmap - Zenmap

TASK 1.2

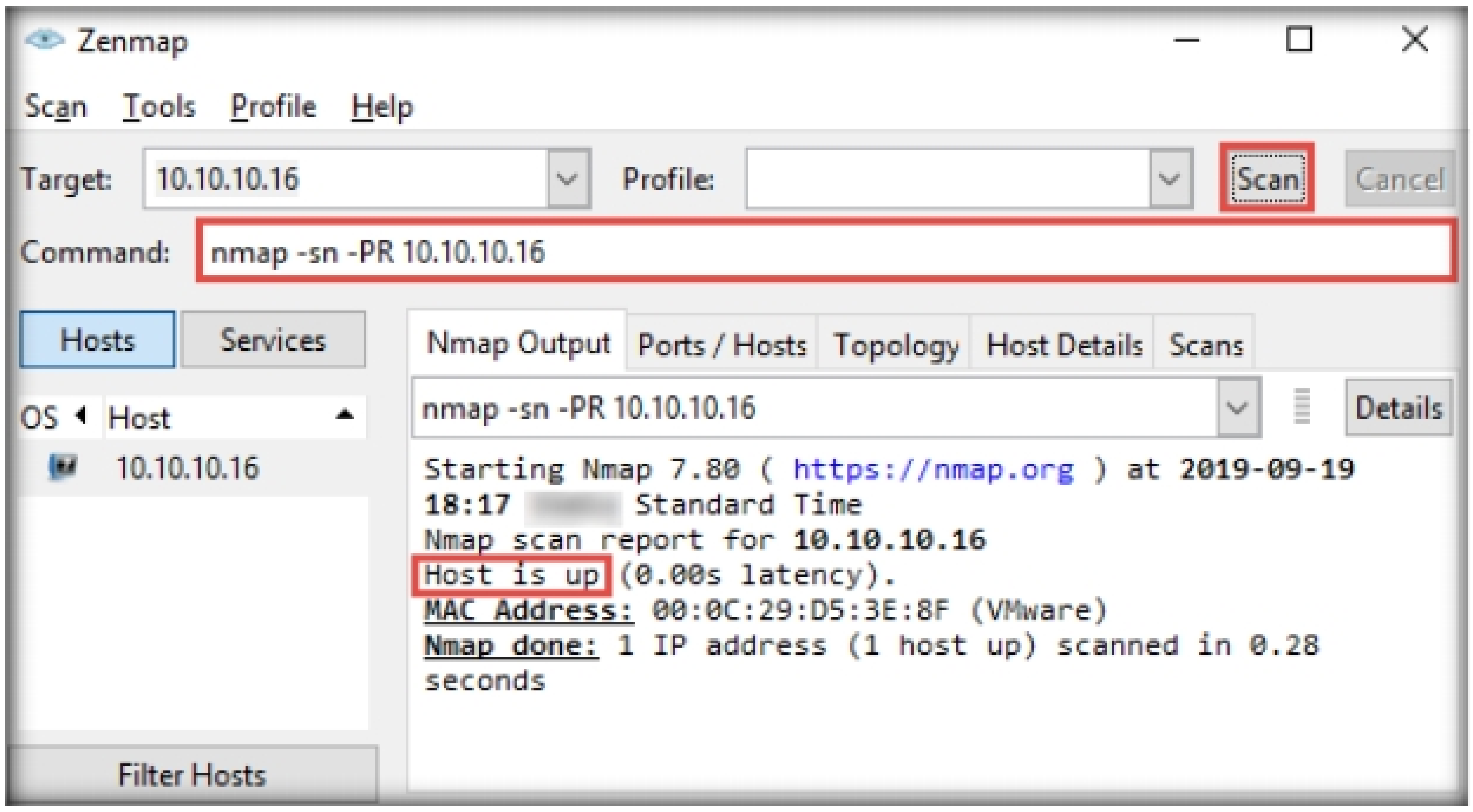
Perform ARP Ping Scan

7. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sn -PR <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sn**: disables port scan and **-PR**: performs ARP ping scan.

8. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: In this lab, we are targeting the **Windows Server 2016** (**10.10.10.16**) virtual machine.


Zenmap
Scan
Tools
Profile
Help
Target:
Profile:
Scan
Cancel
Command:
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
10.10.10.16
Details
Filter Hosts

Target: 10.10.10.16

Command: nmap -sn -PR 10.10.10.16

```
nmap -sn -PR 10.10.10.16
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-19
18:17 [redacted] Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
MAC Address: 00:0C:29:D5:3E:8F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.28
seconds
```

Figure 1.1.4: Zenmap scan results for ARP ping scan

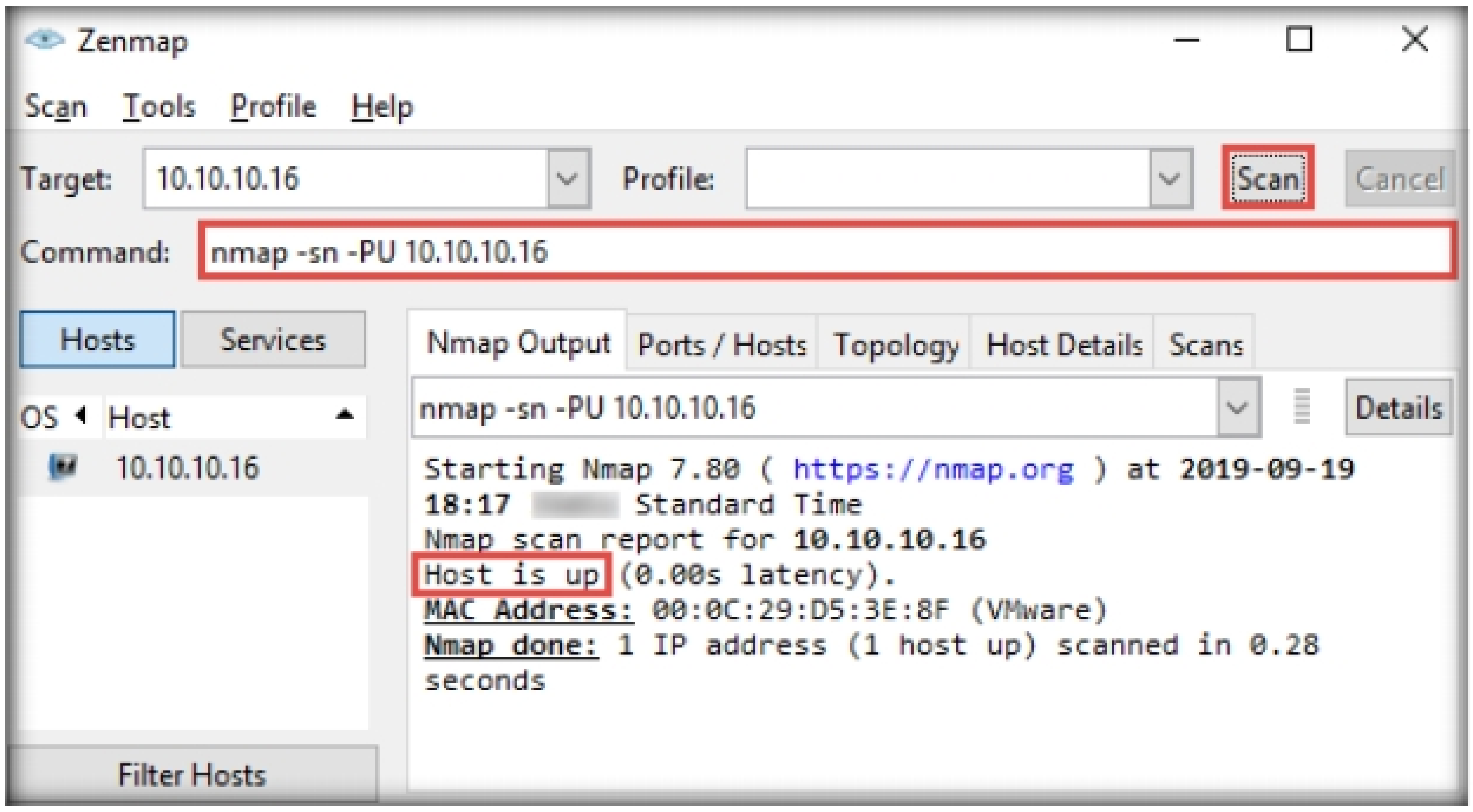
Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

TASK 1.3

Perform UDP Ping Scan

9. In the **Command** field, type **nmap -sn -PU <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: **-PU**: performs the UDP ping scan.


Zenmap
Scan
Tools
Profile
Help
Profile:
Scan
Cancel
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

Target: 10.10.10.16

Command: nmap -sn -PU 10.10.10.16

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-19
18:17 [redacted] Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
MAC Address: 00:0C:29:D5:3E:8F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.28
seconds
```

Figure 1.1.5: Zenmap scan results for UDP ping scan

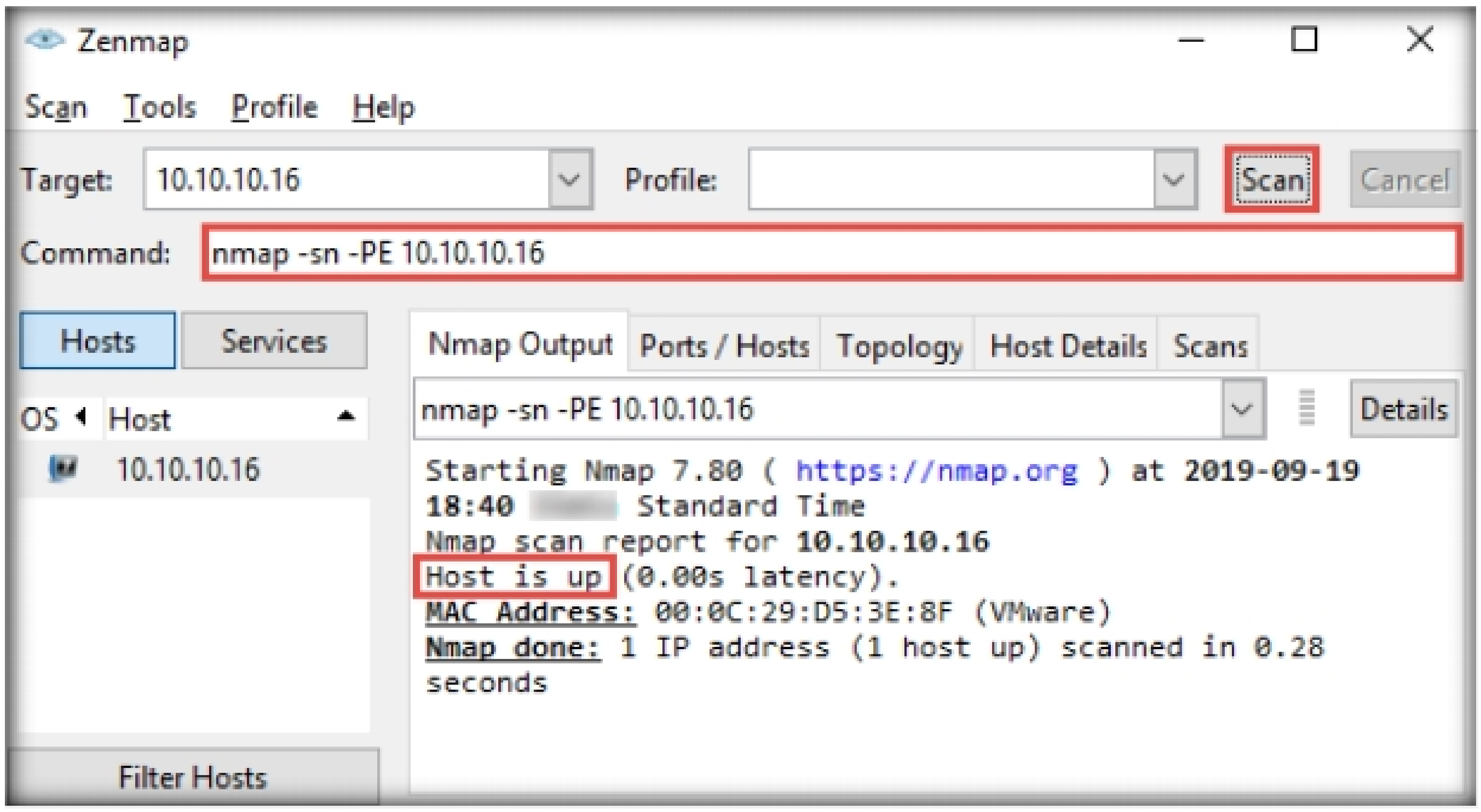
Note: The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.

TASK 1.4

Perform ICMP ECHO Ping Scan

10. Now, we will perform the ICMP ECHO ping scan. In the **Command** field, type **nmap -sn -PE <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: **-PE**: performs the ICMP ECHO ping scan.


Zenmap
Scan
Tools
Profile
Help
Profile:
Scan
Cancel
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

Target: 10.10.10.16

Command: nmap -sn -PE 10.10.10.16

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-19
18:40 [redacted] Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
MAC Address: 00:0C:29:D5:3E:8F (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.28
seconds
```

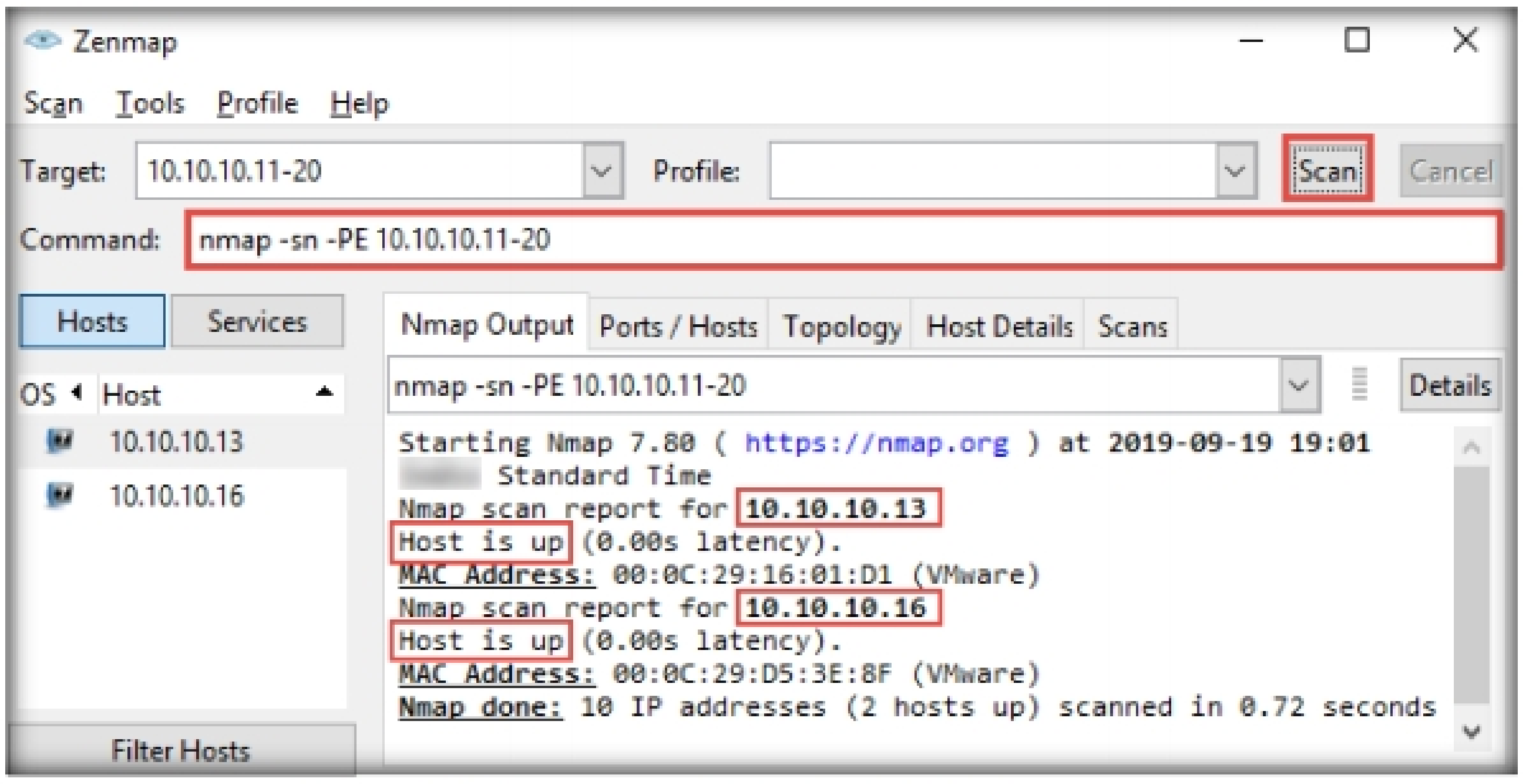
Figure 1.1.6: Zenmap scan results for ICMP ECHO ping scan

Note: The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.

TASK 1.5

Perform ICMP ECHO Ping Sweep

11. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the **Command** field, type **nmap -sn -PE <Target Range of IP Addresses>** (here, the target range of IP addresses is **10.10.10.11-20**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot



Target: 10.10.10.11-20

Command: nmap -sn -PE 10.10.10.11-20

10.10.10.13
10.10.10.16

```
nmap -sn -PE 10.10.10.11-20
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-19 19:01
[redacted] Standard Time
Nmap scan report for 10.10.10.13
Host is up (0.00s latency).
MAC Address: 00:0C:29:16:01:D1 (VMware)
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
MAC Address: 00:0C:29:D5:3E:8F (VMware)
Nmap done: 10 IP addresses (2 hosts up) scanned in 0.72 seconds
```

Figure 1.1.7: Zenmap scan results for ICMP ECHO ping sweep scan

Note: The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.

12. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

    - **ICMP Timestamp and Address Mask Ping Scan**: These techniques are alternatives for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

      Example –

      ICMP timestamp ping scan

      # nmap -sn -PP <target IP address>

      ICMP address mask ping scan

      # nmap -sn -PM <target IP address>

    - **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

      # nmap -sn -PS <target IP address>

    - **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

      # nmap -sn -PA <target IP address>

- **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

```
# nmap -sn -PO <target IP address>
```

13. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
14. Close all open windows and document all the acquired information.

TASK 2

Perform Host Discovery using Angry IP Scanner

Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

1. Turn on the **Ubuntu** virtual machine.

Note: Ensure that the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines are turned on.

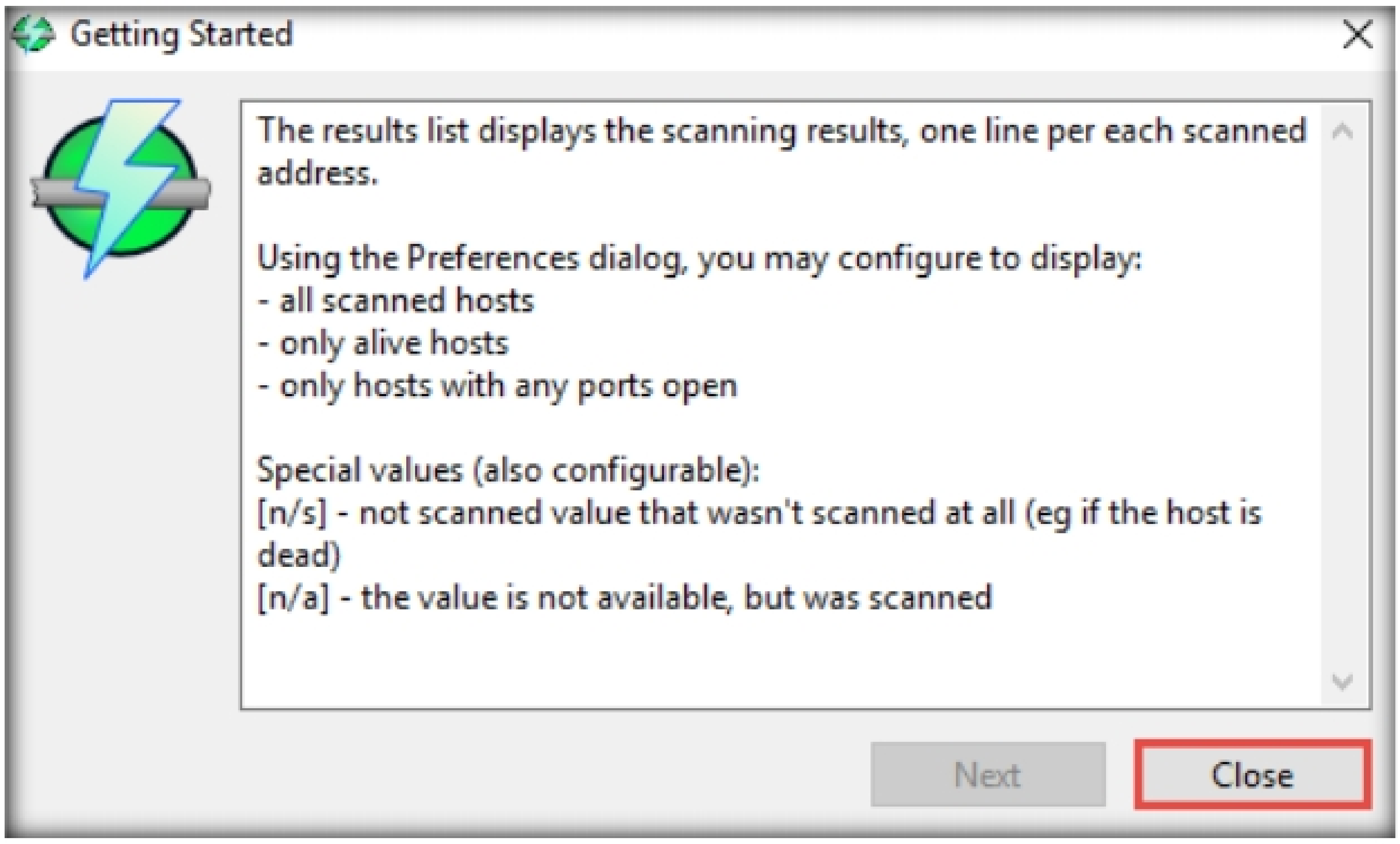
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner** and double-click **ipscan-win64-3.6.1.exe**.

TASK 2.1

Install Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins

3. Angry IP Scanner starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.



The results list displays the scanning results, one line per each scanned address.

Using the Preferences dialog, you may configure to display:
- all scanned hosts
- only alive hosts
- only hosts with any ports open

Special values (also configurable):
[n/s] - not scanned value that wasn't scanned at all (eg if the host is dead)
[n/a] - the value is not available, but was scanned

Figure 1.2.1: Getting Started window

4. The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.

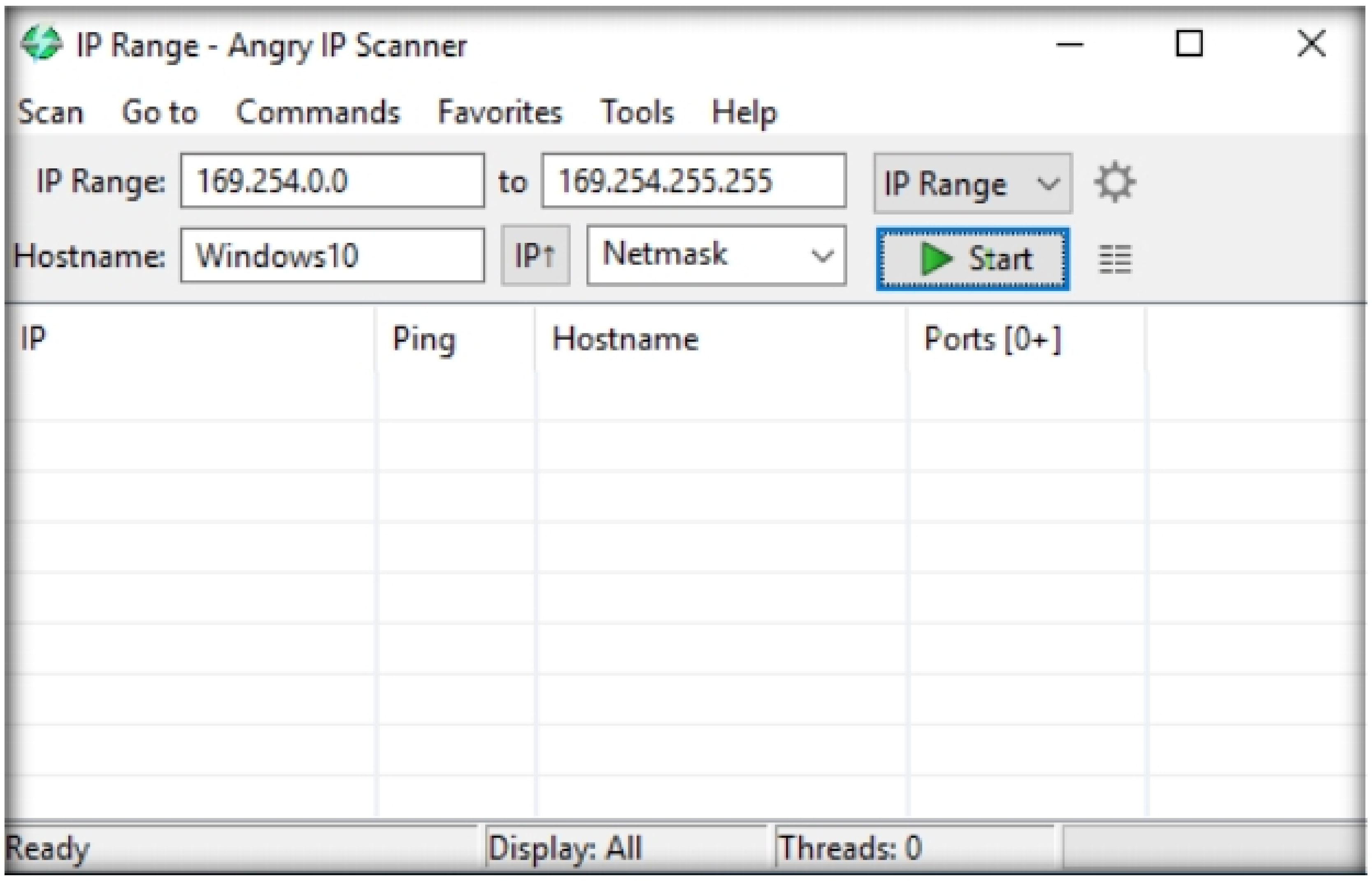

IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 169.254.0.0 to 169.254.255.255
IP Range
Hostname: Windows10
IP↑
Netmask
Start
IP
Ping
Hostname
Ports [0+]
Ready
Display: All
Threads: 0

Figure 1.2.2: IP Range - Angry IP Scanner Window

TASK 2.2

Perform the Scan

5. In the **IP Range** fields, type the IP range as **10.10.10.0** to **10.10.10.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.

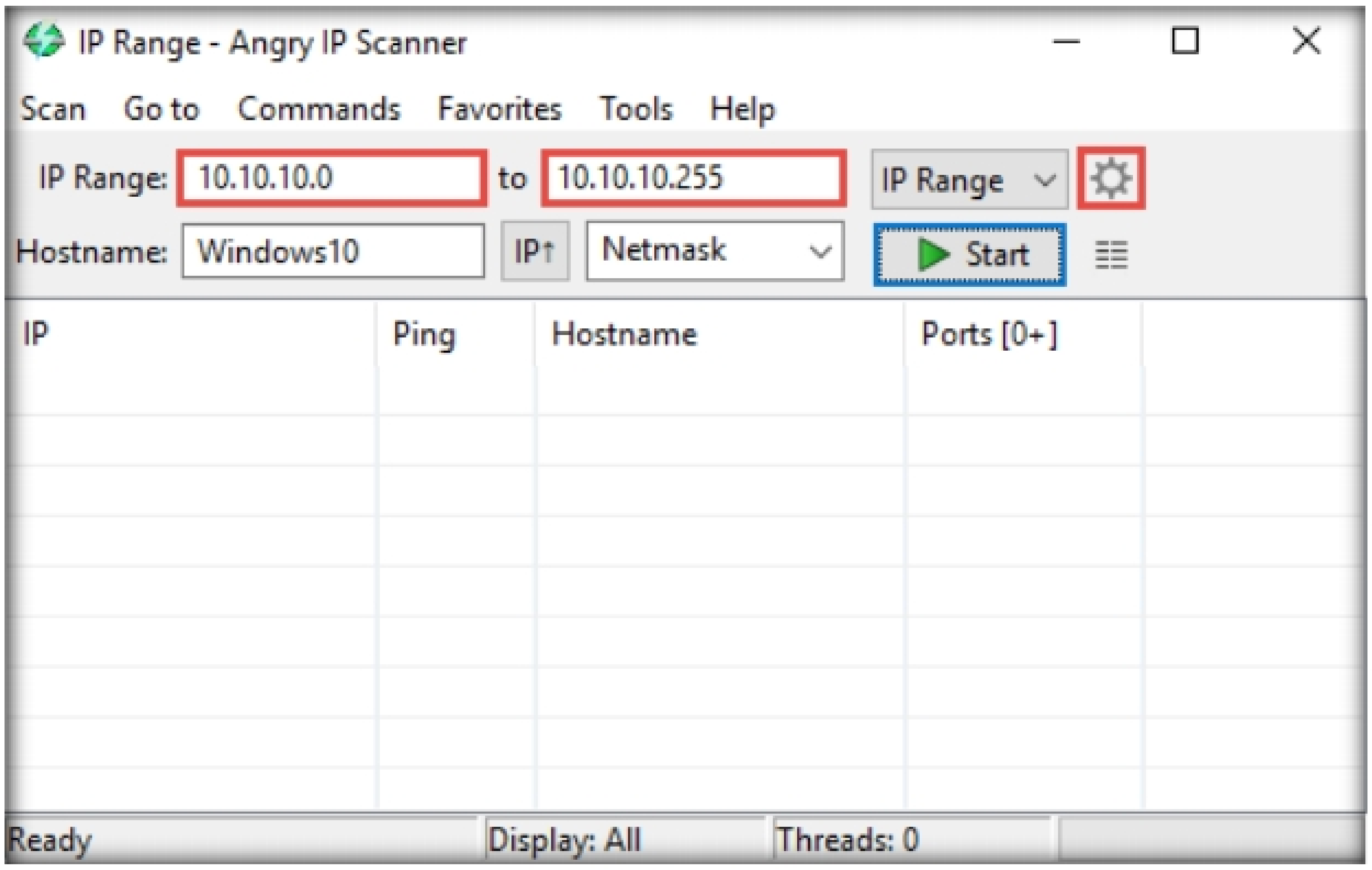
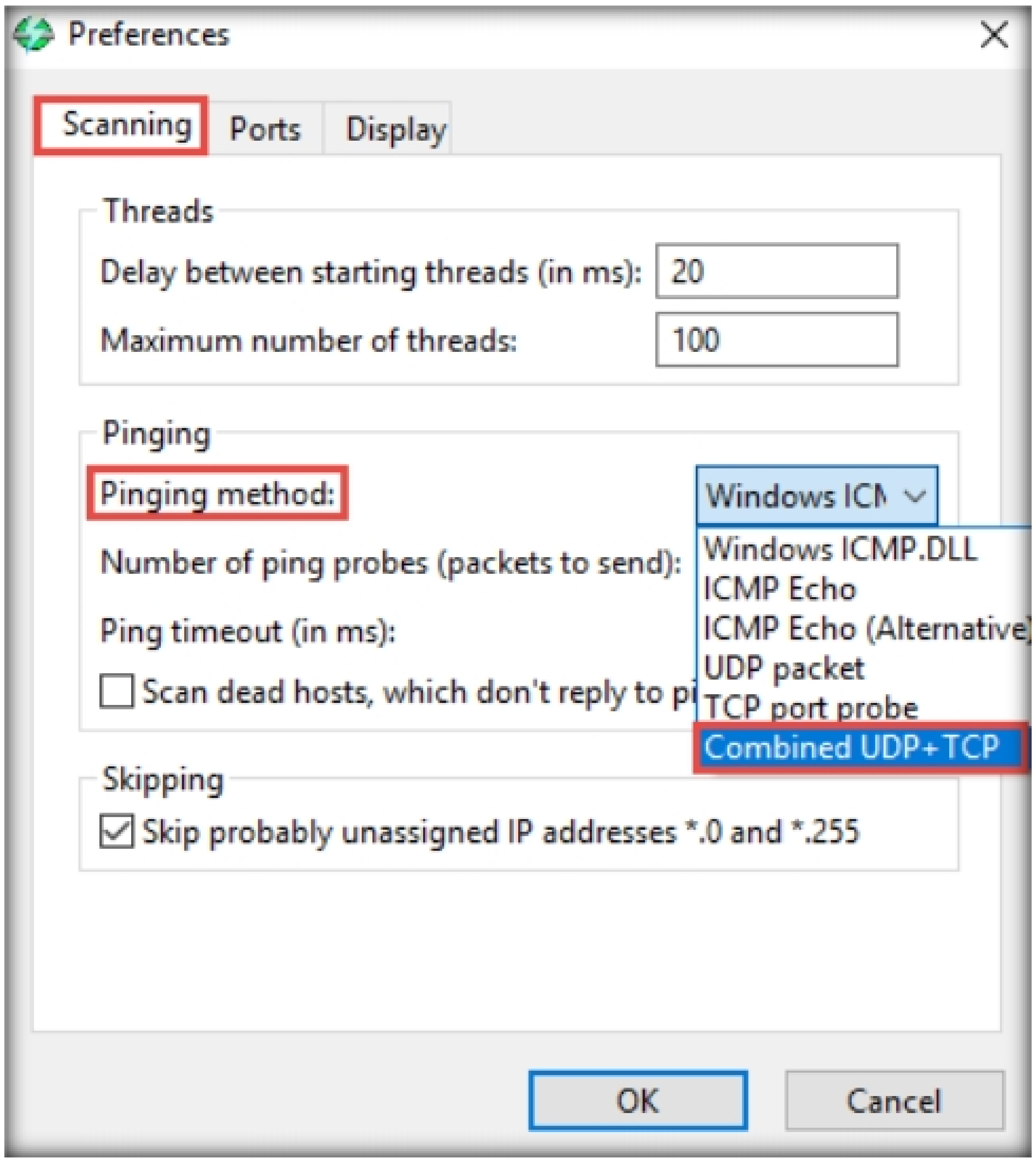

IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 10.10.10.0 to 10.10.10.255
IP Range
Hostname: Windows10
IP↑
Netmask
Start
IP
Ping
Hostname
Ports [0+]
Ready
Display: All
Threads: 0

Figure 1.2.3: Filling the IP range

6. The **Preferences** window appears. In the **Scanning** tab, under the **Pinging** section, select the **Pinging method** as **Combined UDP+TCP** from the drop-down list.



Threads

Delay between starting threads (in ms): 20

Maximum number of threads: 100

Pinging

Pinging method: Windows ICM

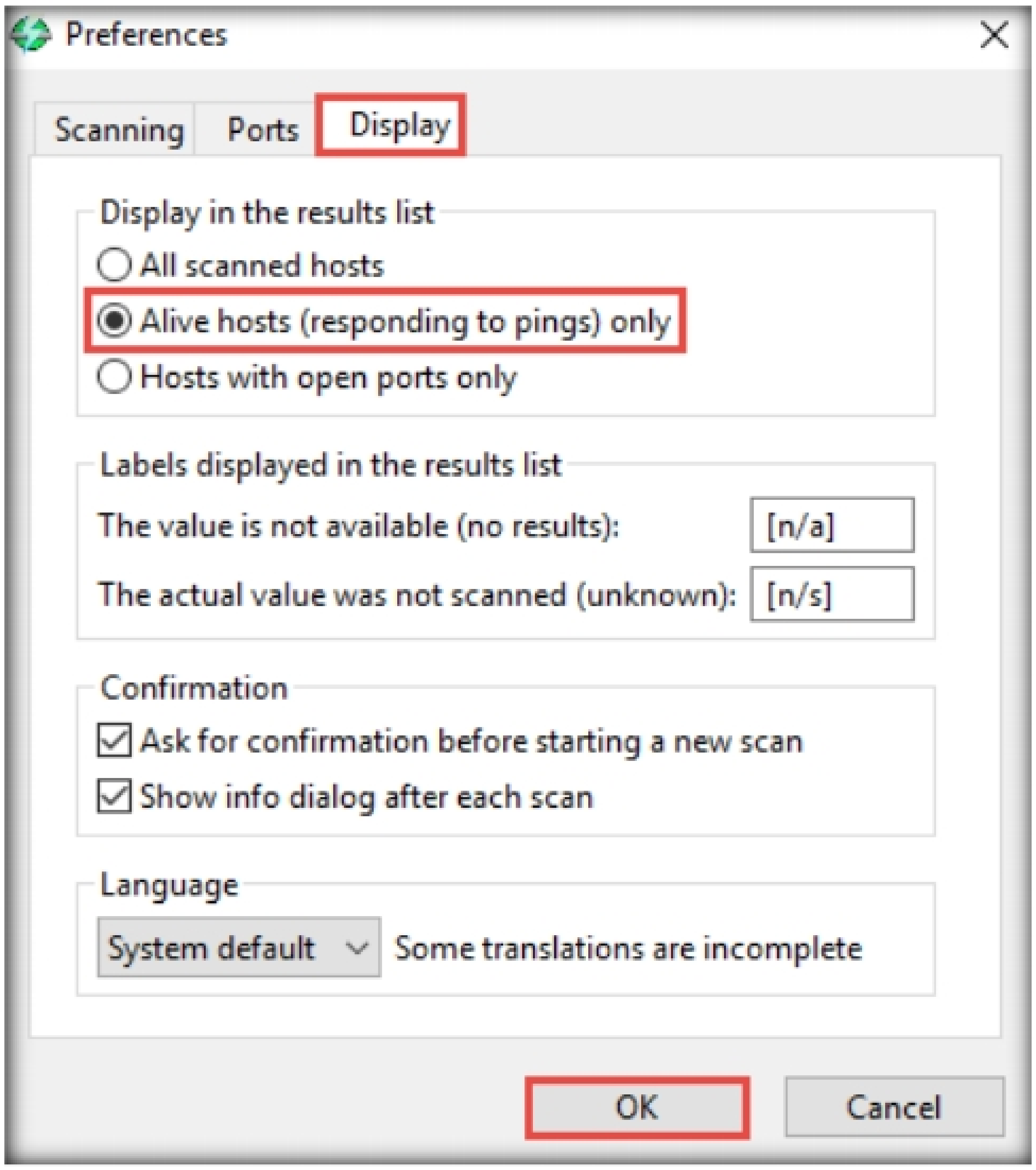
Skipping

☑ Skip probably unassigned IP addresses *.0 and *.255

Preferences
Scanning
Ports
Display
Number of ping probes (packets to send):
Ping timeout (in ms):
☐ Scan dead hosts, which don't reply to pi
Windows ICMP.DLL
ICMP Echo
ICMP Echo (Alternative)
UDP packet
TCP port probe
Combined UDP+TCP
OK
Cancel

Figure 1.2.4: Angry IP Scanner Preferences window

7. Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.


Preferences
Scanning
Ports
Display
OK
Cancel

Display in the results list
○ All scanned hosts
● Alive hosts (responding to pings) only
○ Hosts with open ports only

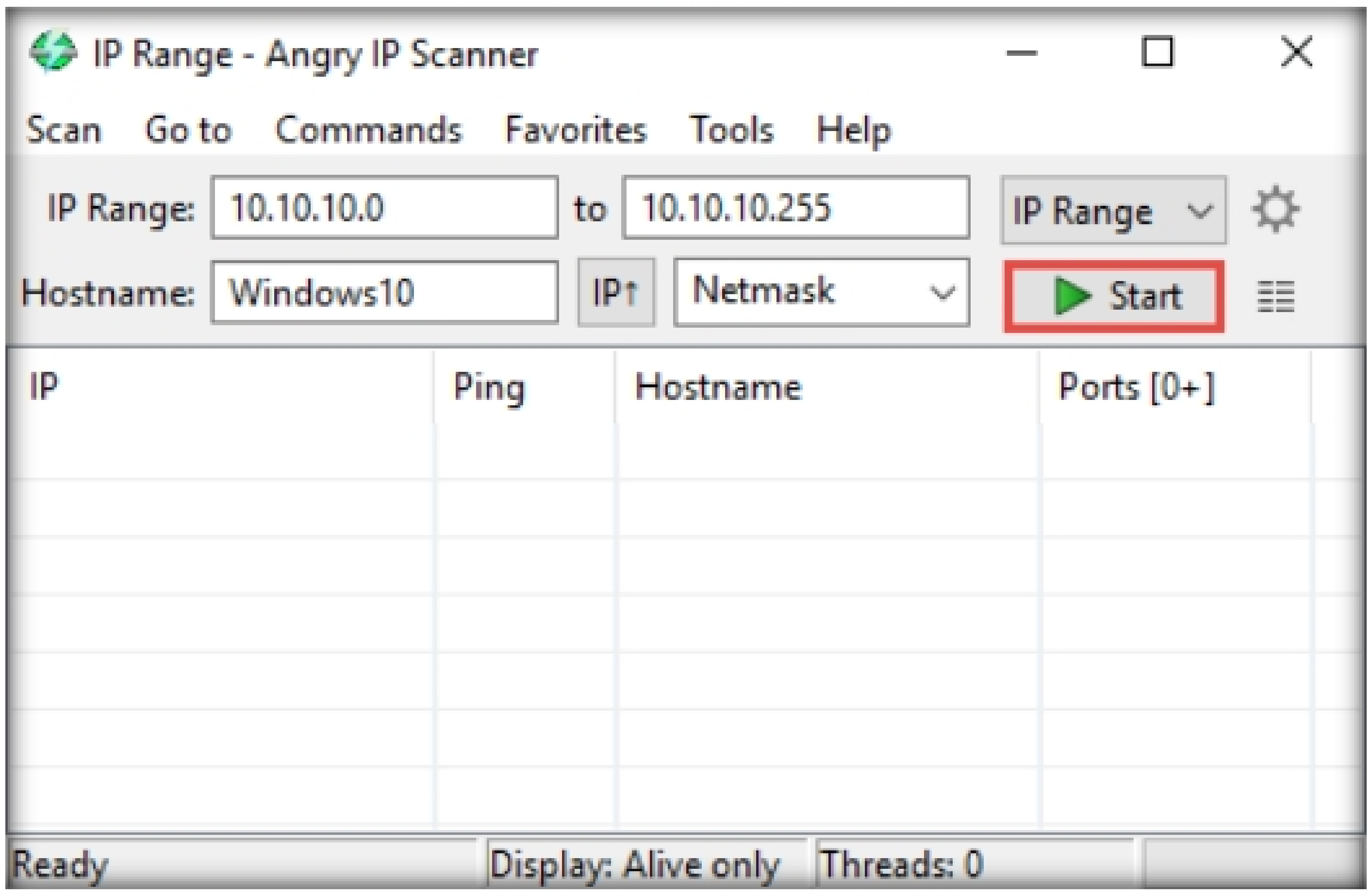
Labels displayed in the results list
The value is not available (no results): [n/a]
The actual value was not scanned (unknown): [n/s]

Confirmation
☑ Ask for confirmation before starting a new scan
☑ Show info dialog after each scan

Language
System default — Some translations are incomplete

Figure 1.2.5: Display tab options in the preferences window

8. In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.


IP Range - Angry IP Scanner
Scan
Go to
Commands
Favorites
Tools
Help
IP↑
IP Range
Start
IP
Ping
Hostname
Ports [0+]

IP Range: 10.10.10.0 to 10.10.10.255
Hostname: Windows10
Netmask

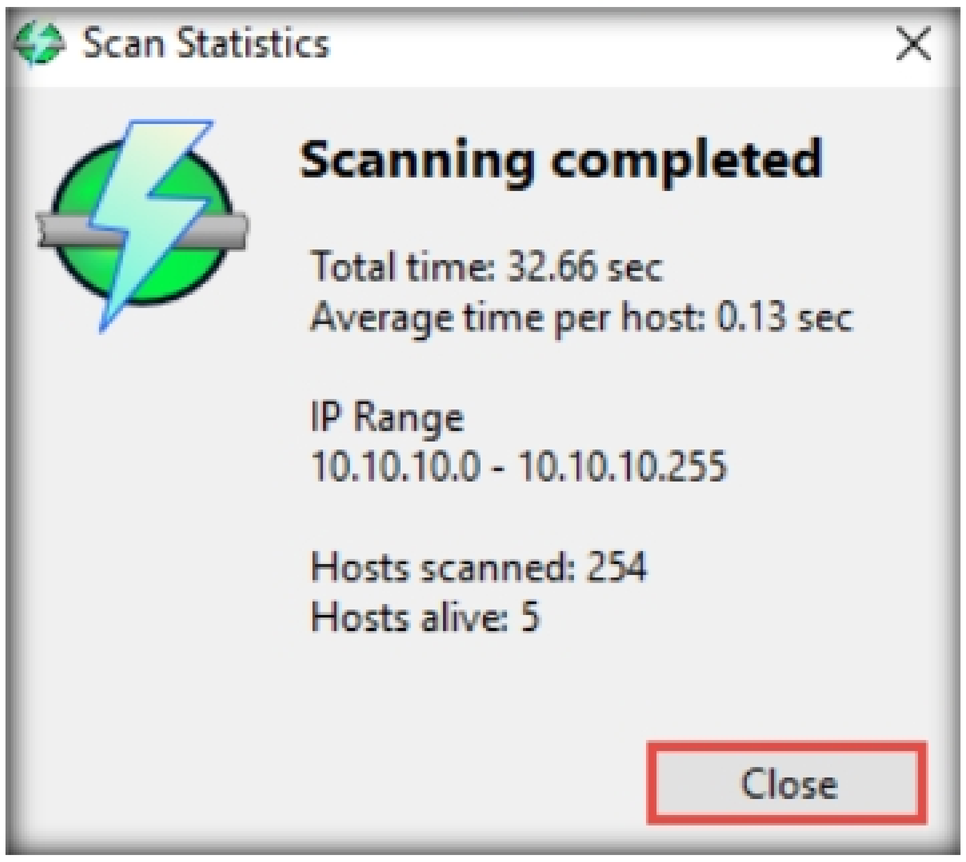
Ready | Display: Alive only | Threads: 0

Figure 1.2.6: Starting the scan

9. **Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found. Check the progress bar on the bottom-right corner to see the progress of the scanning.

Note: IP addresses may differ in your lab environment.

10. After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 6) and click **Close**.



Scanning completed

Total time: 32.66 sec
Average time per host: 0.13 sec

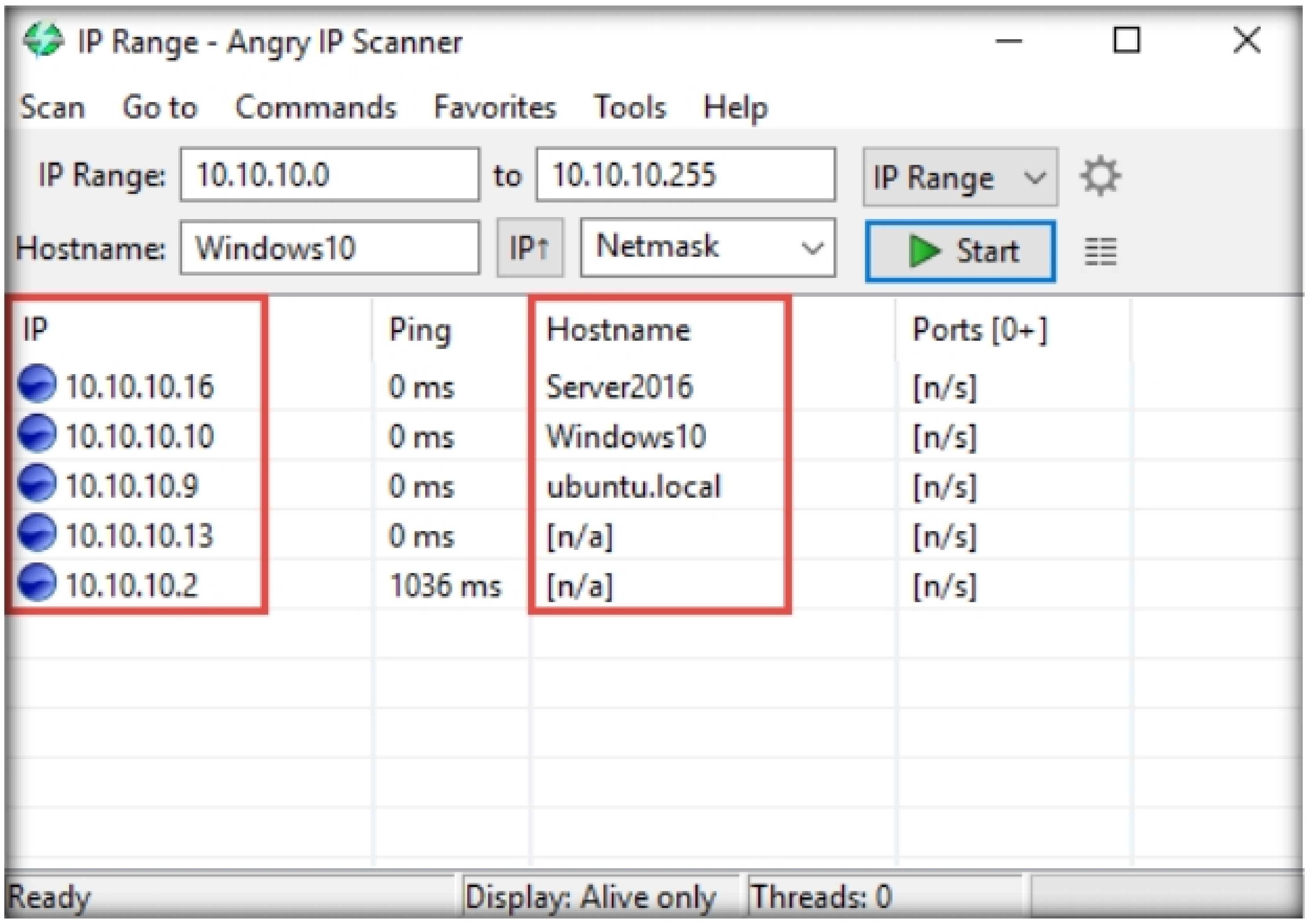
IP Range
10.10.10.0 - 10.10.10.255

Hosts scanned: 254
Hosts alive: 5

Figure 1.2.7: Scanning Completed prompt

You can also use other ping sweep tools such as **SolarWinds Engineer's Toolset** (https://www.solarwinds.com), **NetScanTools Pro** (https://www.netscantools.com), **Colasoft Ping Tool** (https://www.colasoft.com), **Visual Ping Tester** (http://www.pingtester.net), and **OpUtils** (https://www.manageengine.com) to discover active hosts in the target network

11. The results of the scan appear in the **IP Range - Angry IP Scanner** window. You can see all active IP addresses with their hostnames listed in the main window.



IP Range: 10.10.10.0 to 10.10.10.255 IP Range
Hostname: Windows10 Netmask

IP	Ping	Hostname	Ports [0+]
10.10.10.16	0 ms	Server2016	[n/s]
10.10.10.10	0 ms	Windows10	[n/s]
10.10.10.9	0 ms	ubuntu.local	[n/s]
10.10.10.13	0 ms	[n/a]	[n/s]
10.10.10.2	1036 ms	[n/a]	[n/s]

Ready Display: Alive only Threads: 0

Figure 1.2.8: Scan results

12. This concludes the demonstration of discovering alive hosts in the target range of IP addresses using various Angry IP Scanner.
13. Close all open windows and document all the acquired information.
14. Turn off all the virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ **Yes**	☑ **No**
Platform Supported	
☑ **Classroom**	☑ **iLabs**

Lab

2

Perform Port and Service Discovery

Port and service discovery is the process of identifying open ports and services running on the target IP addresses/active hosts.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering active hosts in the target network is to scan for open ports and services running on the target IP addresses in the target network. This discovery of open ports and services can be performed by using various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- MegaPing located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing**

- NetScanTools Pro located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 40 Minutes

Overview of Port and Service Discovery

Port scanning techniques are categorized according to the type of protocol used for communication within the network.

- **TCP Scanning**
  - Open TCP scanning methods (TCP connect/full open scan)
  - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- **UDP Scanning**
- **SCTP Scanning**
  - SCTP INIT Scanning
  - SCTP COOKIE/ECHO Scanning
- **SSDP and List Scanning**
- **IPv6 Scanning**

Lab Tasks

TASK 1

Perform Port and Service Discovery using MegaPing

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines.

TASK 1.1

Install MegaPing

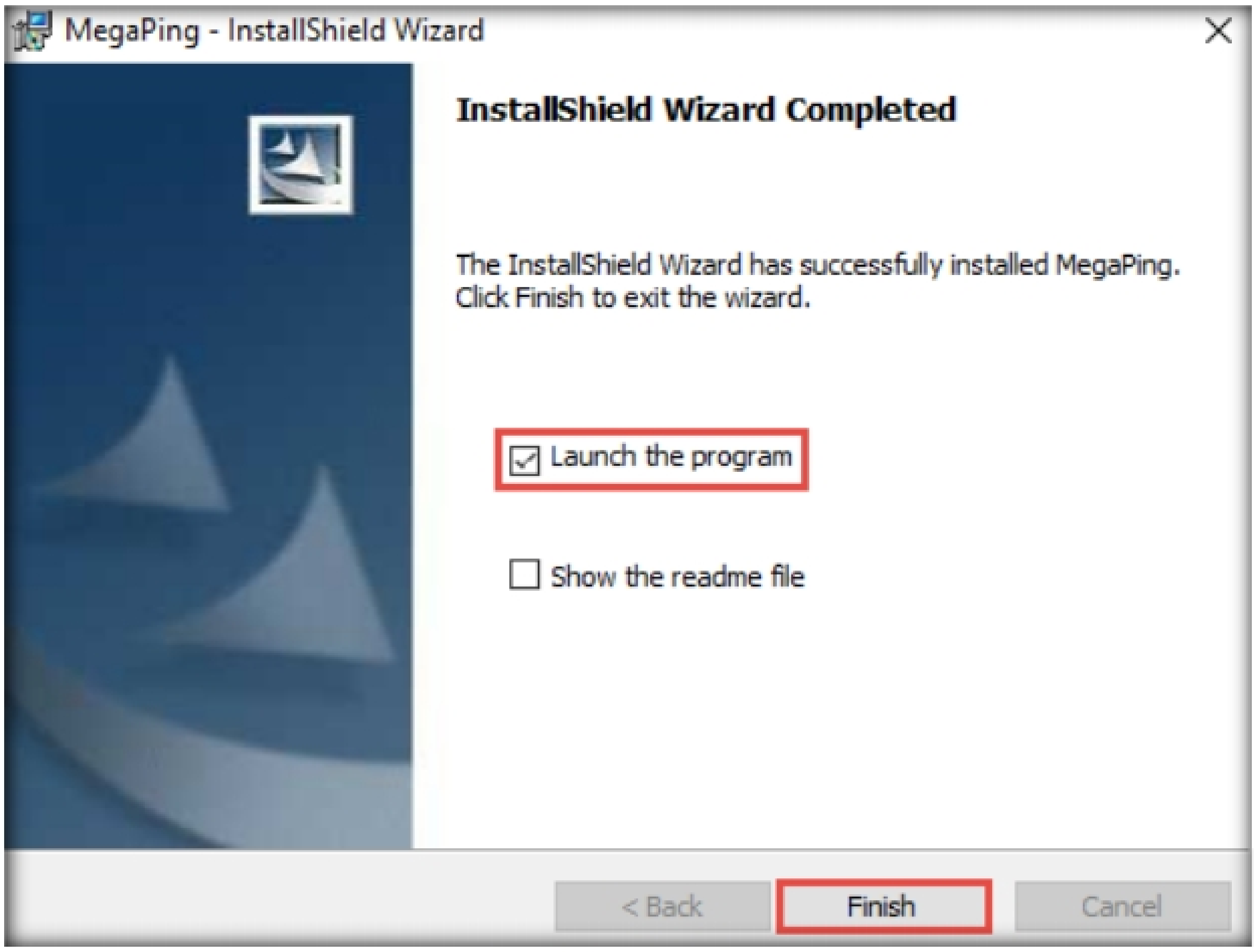
2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc.

5. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.



MegaPing - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed MegaPing.
Click Finish to exit the wizard.

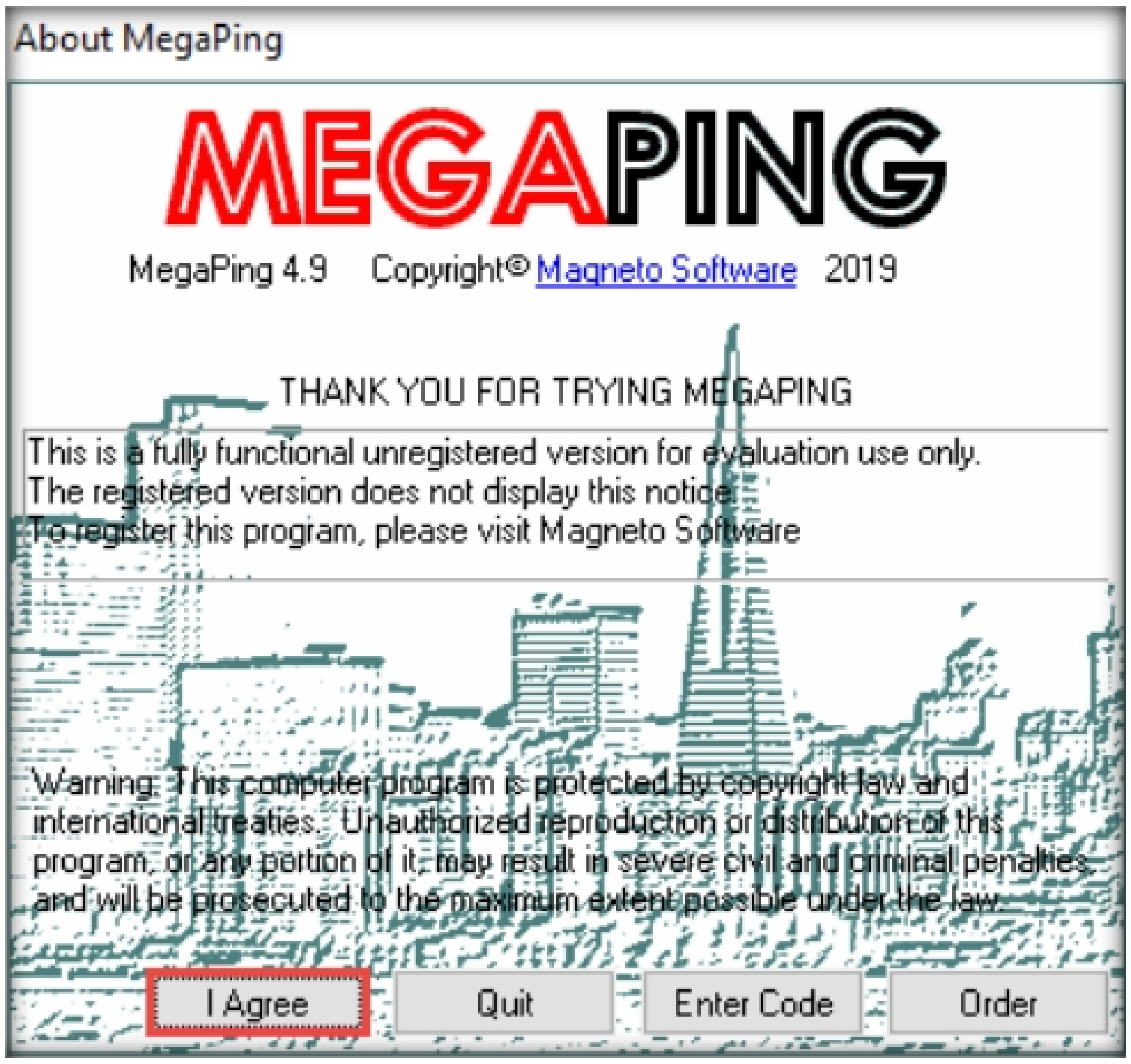
☑ Launch the program

☐ Show the readme file

Figure 2.1.1: Launching MegaPing from Start menu

You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

6. The **About MegaPing** window appears; click the **I Agree** button.



About MegaPing

MEGAPING

MegaPing 4.9 Copyright© Magneto Software 2019

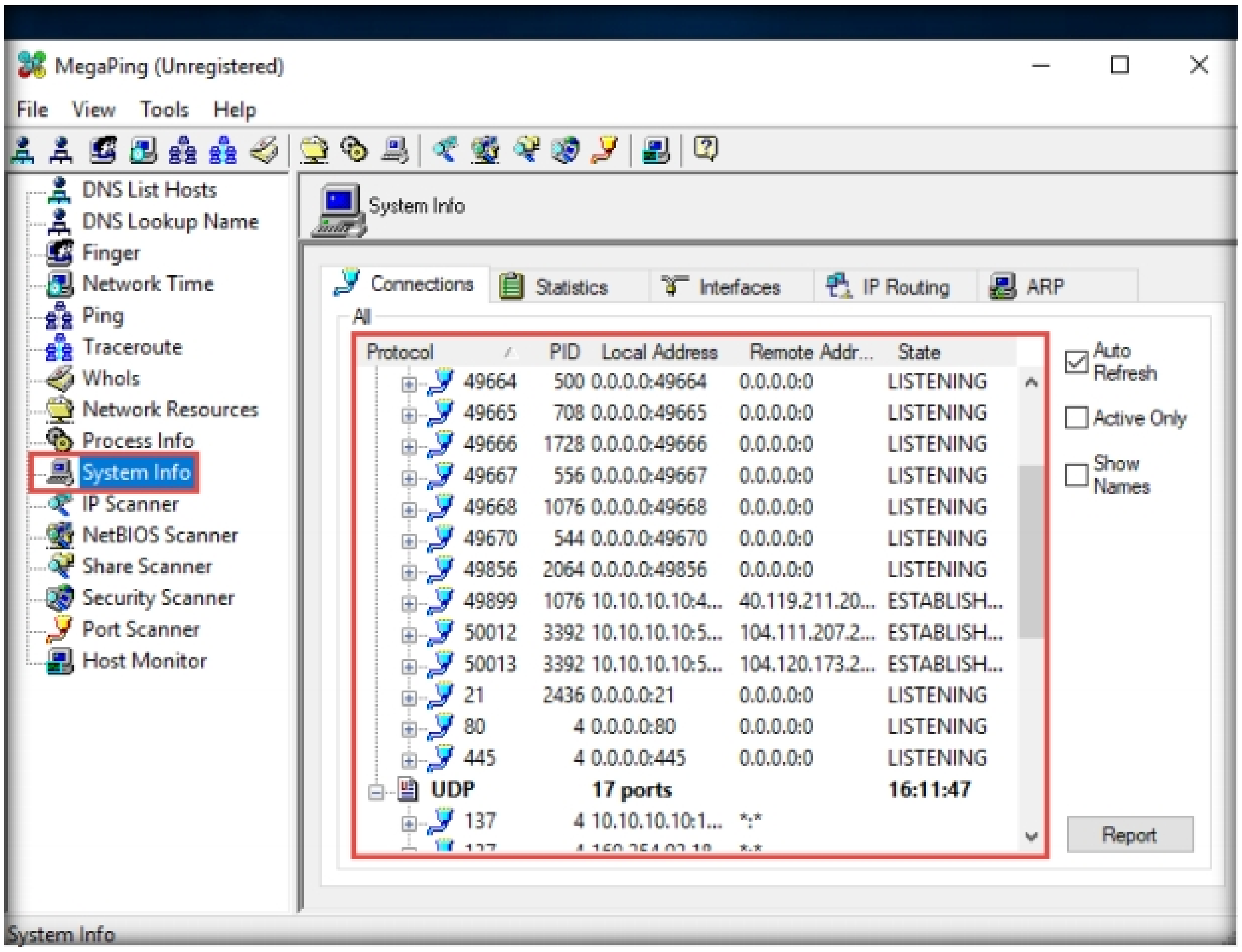
THANK YOU FOR TRYING MEGAPING

This is a fully functional unregistered version for evaluation use only.
The registered version does not display this notice.
To register this program, please visit Magneto Software

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 2.1.2: About MegaPing pop-up

7. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.


MegaPing (Unregistered)
File
View
Tools
Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
System Info
Connections
Statistics
Interfaces
IP Routing
ARP
All
Report
System Info

Protocol	PID	Local Address	Remote Addr...	State
49664	500	0.0.0.0:49664	0.0.0.0:0	LISTENING
49665	708	0.0.0.0:49665	0.0.0.0:0	LISTENING
49666	1728	0.0.0.0:49666	0.0.0.0:0	LISTENING
49667	556	0.0.0.0:49667	0.0.0.0:0	LISTENING
49668	1076	0.0.0.0:49668	0.0.0.0:0	LISTENING
49670	544	0.0.0.0:49670	0.0.0.0:0	LISTENING
49856	2064	0.0.0.0:49856	0.0.0.0:0	LISTENING
49899	1076	10.10.10.10:4...	40.119.211.20...	ESTABLISH...
50012	3392	10.10.10.10:5...	104.111.207.2...	ESTABLISH...
50013	3392	10.10.10.10:5...	104.120.173.2...	ESTABLISH...
21	2436	0.0.0.0:21	0.0.0.0:0	LISTENING
80	4	0.0.0.0:80	0.0.0.0:0	LISTENING
445	4	0.0.0.0:445	0.0.0.0:0	LISTENING
UDP		**17 ports**		**16:11:47**
137	4	10.10.10.10:1...	*:*	

☑ Auto Refresh
☐ Active Only
☐ Show Names

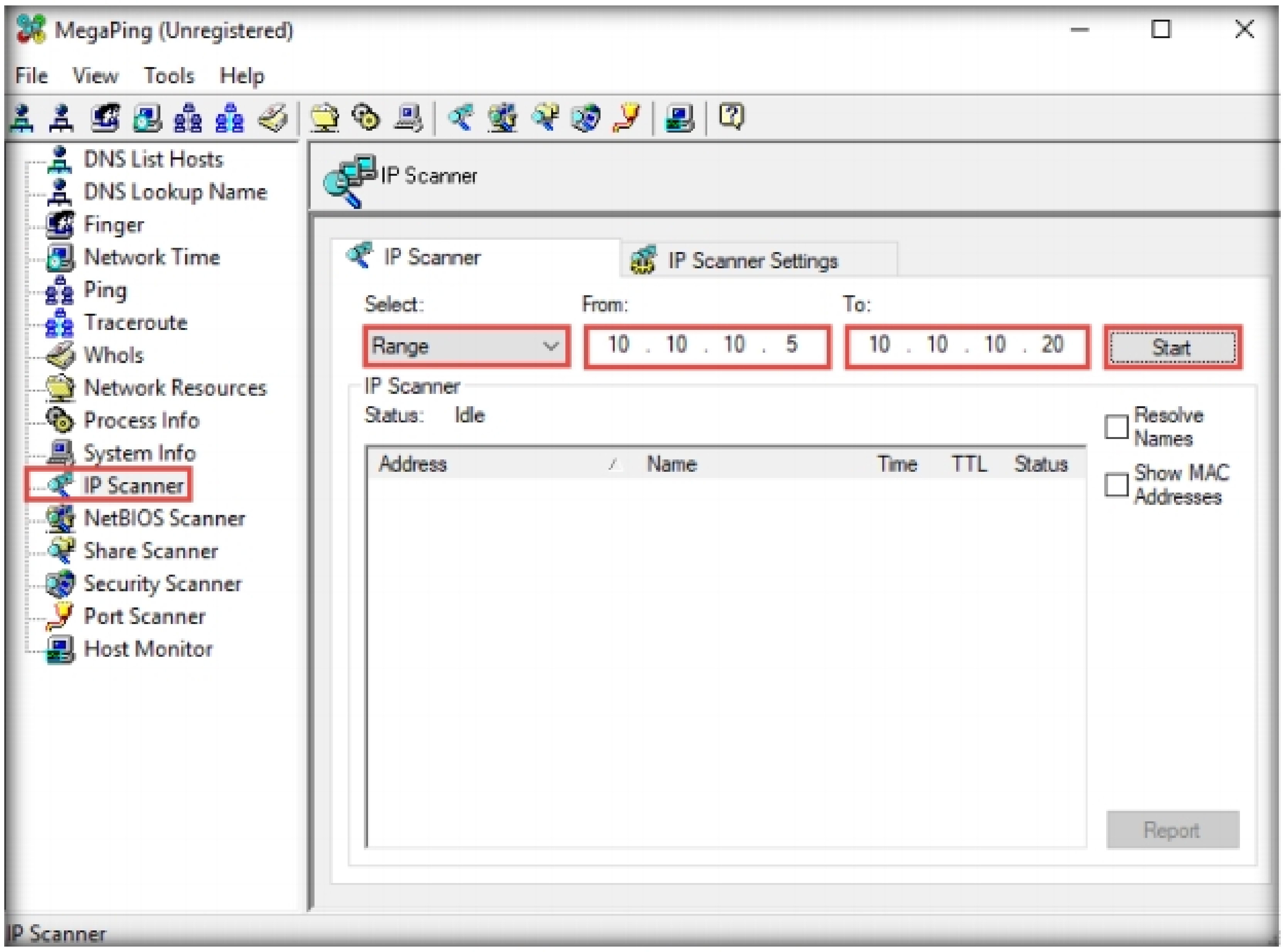
Figure 2.1.3: MegaPing GUI

TASK 1.2

Scan for Live Hosts

8. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.10.5** to **10.10.10.20**; then, click **Start**.

Note: You may specify the IP range depending on your network.


MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
IP Scanner
IP Scanner
IP Scanner Settings
Start
☐ Resolve Names
☐ Show MAC Addresses
Address
Name
Time
TTL
Status
Report
IP Scanner

Select: Range

From: 10 . 10 . 10 . 5

To: 10 . 10 . 10 . 20

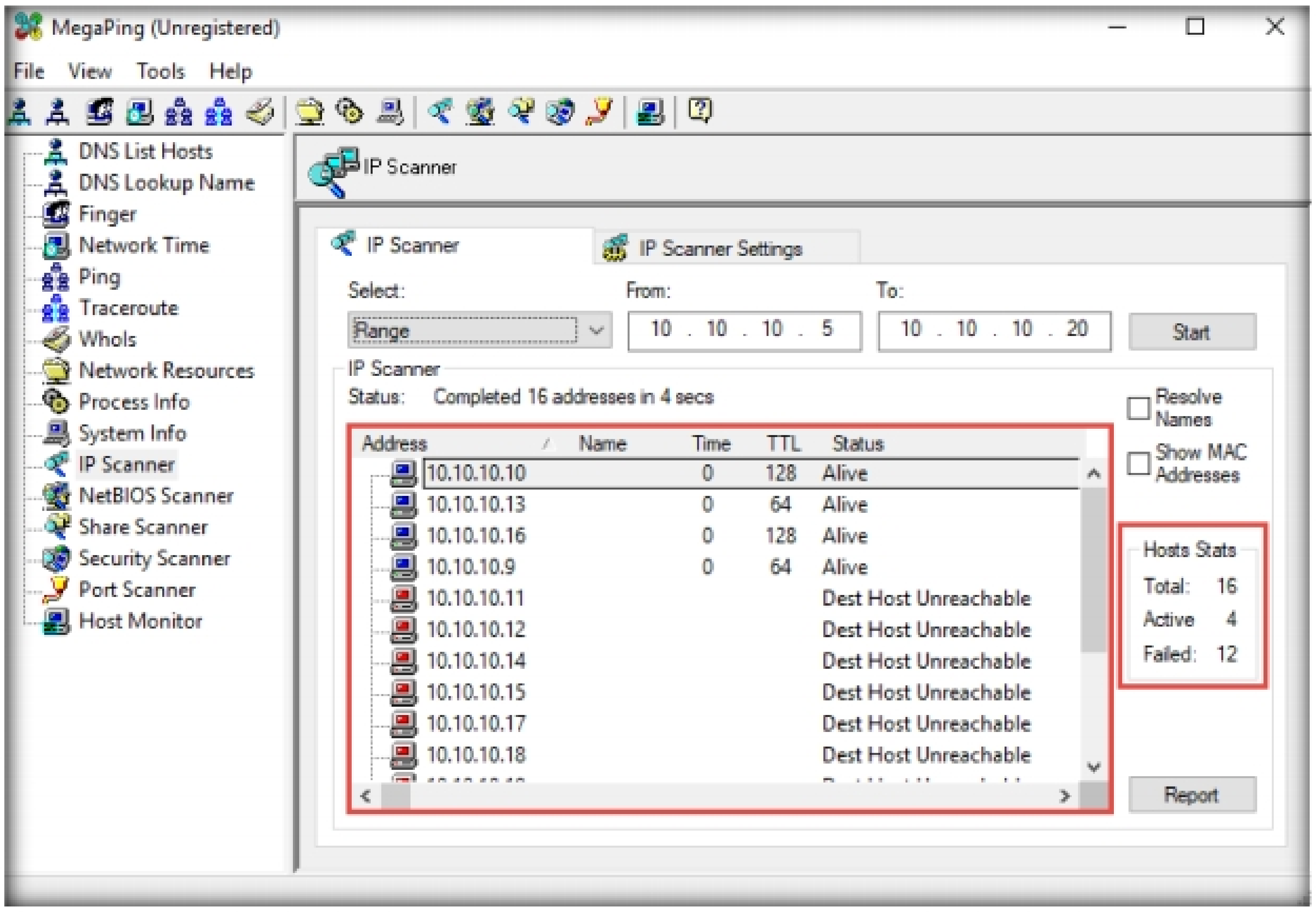
IP Scanner

Status: Idle

Figure 2.1.4: Configuring MegaPing

9. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.

Note: The results may vary in your lab environment.


MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
IP Scanner
IP Scanner
IP Scanner Settings
Start
☐ Resolve Names
☐ Show MAC Addresses
Report

Select: Range

From: 10 . 10 . 10 . 5

To: 10 . 10 . 10 . 20

IP Scanner

Status: Completed 16 addresses in 4 secs

Address	Name	Time	TTL	Status
10.10.10.10		0	128	Alive
10.10.10.13		0	64	Alive
10.10.10.16		0	128	Alive
10.10.10.9		0	64	Alive
10.10.10.11				Dest Host Unreachable
10.10.10.12				Dest Host Unreachable
10.10.10.14				Dest Host Unreachable
10.10.10.15				Dest Host Unreachable
10.10.10.17				Dest Host Unreachable
10.10.10.18				Dest Host Unreachable

Hosts Stats

Total: 16

Active 4

Failed: 12

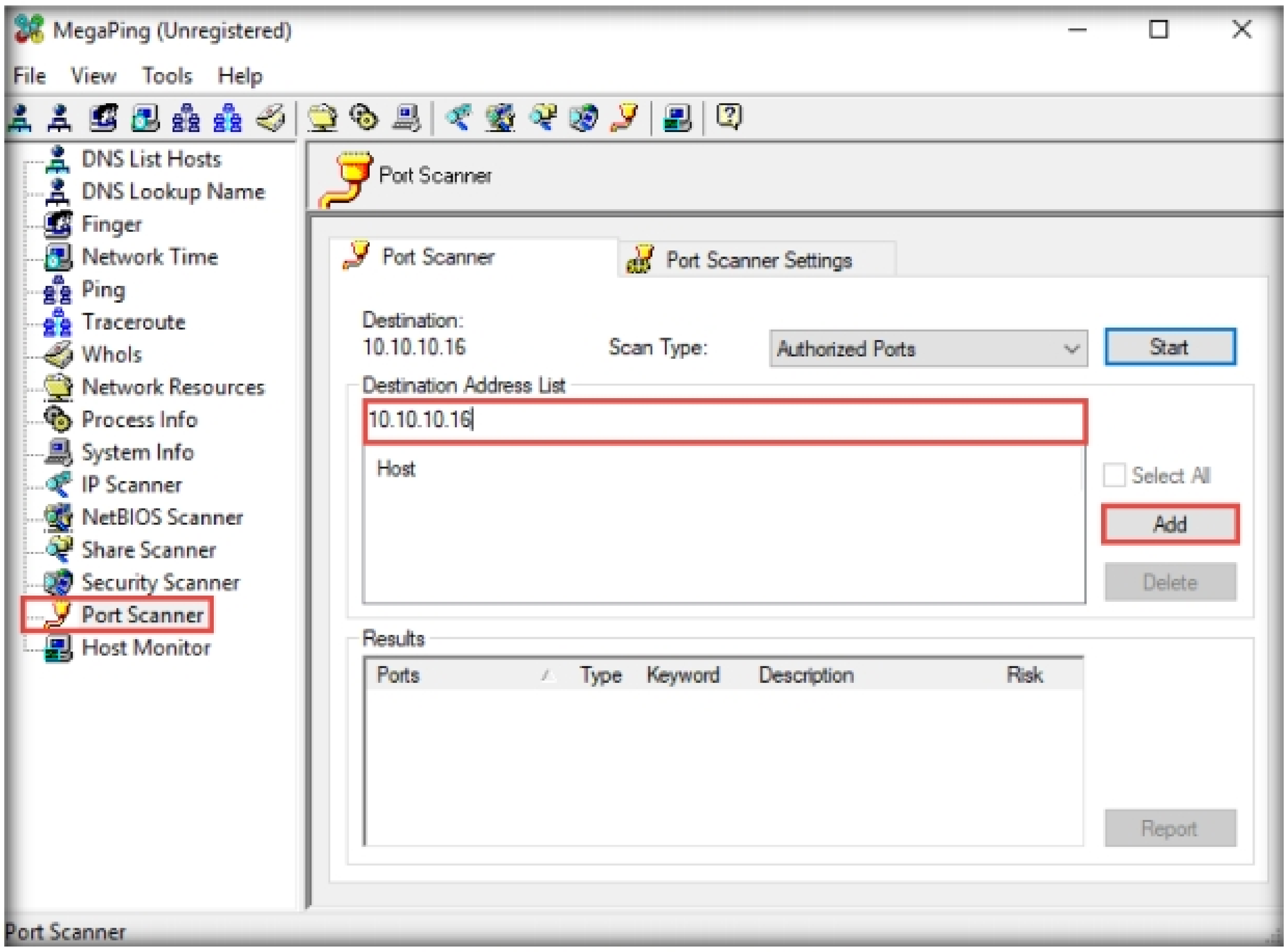
Figure 2.1.5: MegaPing IP Scanning Report

TASK 1.3

Perform Port Scan

10. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016** (**10.10.10.16**) machine into the **Destination Address List** field and click **Add**.

Note: The IP address listed below might vary in your lab environment.


MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
Port Scanner
Port Scanner Settings
Start
Select All
Add
Delete
Results
Ports Type Keyword Description Risk
Report
Port Scanner

Destination: 10.10.10.16

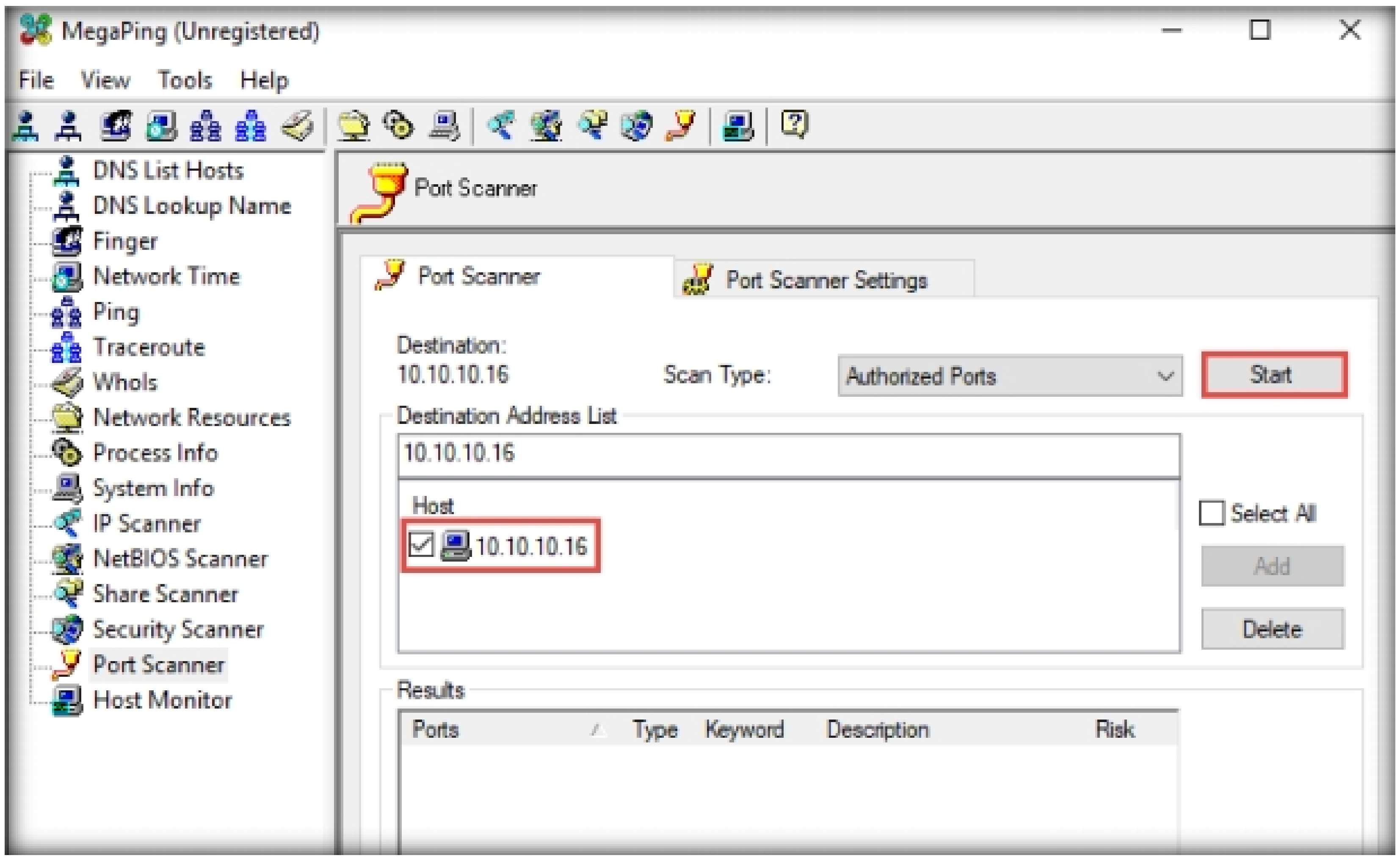
Scan Type: Authorized Ports

Destination Address List: 10.10.10.16

Host

Figure 2.1.6: Adding a host in MegaPing

11. Select the **10.10.10.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.10.16.


MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
Port Scanner
Port Scanner Settings
Start
Select All
Add
Delete
Results
Ports Type Keyword Description Risk

Destination: 10.10.10.16

Scan Type: Authorized Ports

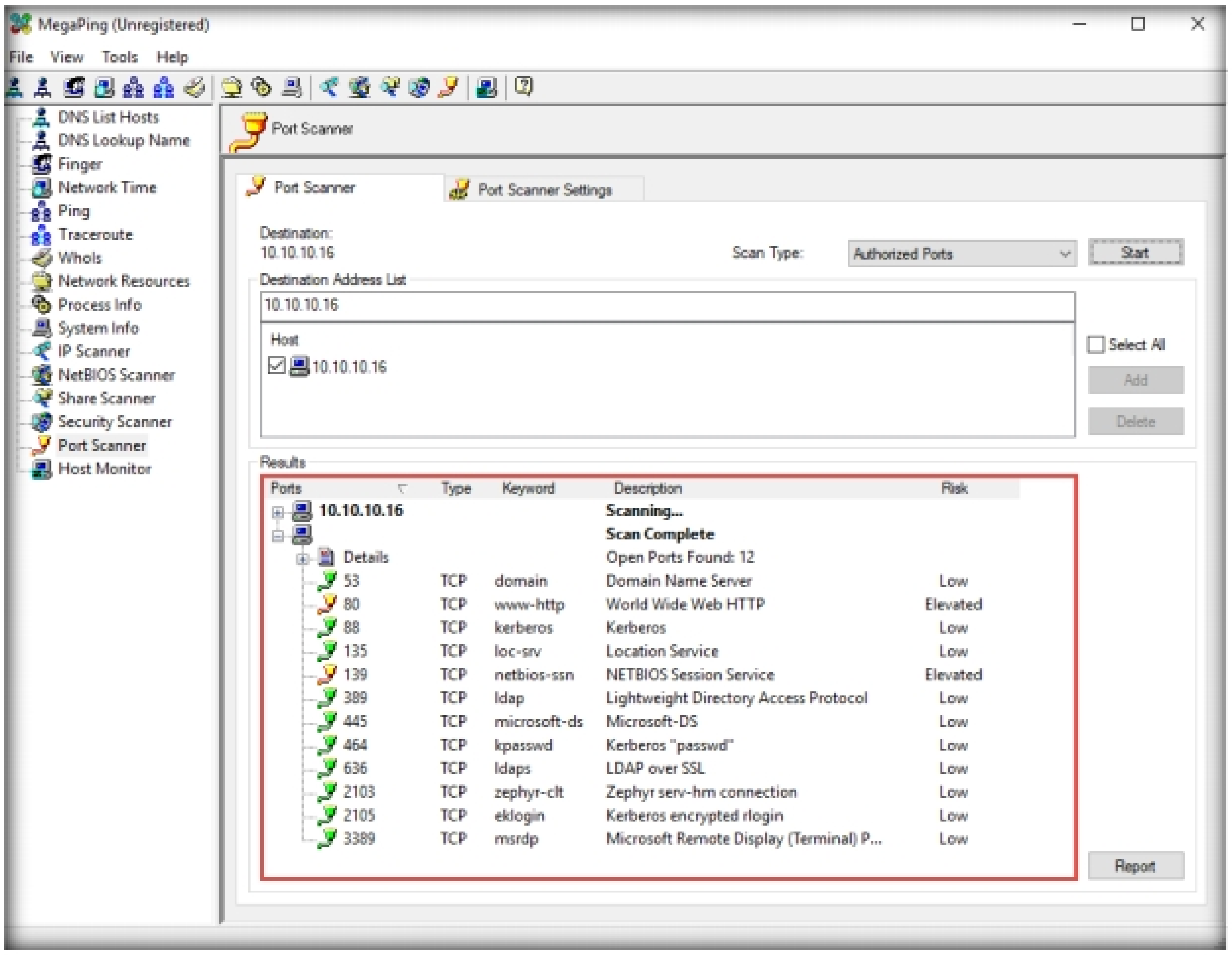
Destination Address List: 10.10.10.16

Host

☑ 10.10.10.16

Figure 2.1.7: Starting MegaPing on the selected host

12. MegaPing lists the ports associated with **Windows Server 2016** (**10.10.10.16**), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot.


MegaPing (Unregistered)
File View Tools Help
DNS List Hosts
DNS Lookup Name
Finger
Network Time
Ping
Traceroute
WhoIs
Network Resources
Process Info
System Info
IP Scanner
NetBIOS Scanner
Share Scanner
Security Scanner
Port Scanner
Host Monitor
Port Scanner
Port Scanner
Port Scanner Settings
Start
Select All
Add
Delete
Report

Destination:
10.10.10.16

Scan Type: Authorized Ports

Destination Address List
10.10.10.16

Host
☑ 10.10.10.16

Results

Ports	Type	Keyword	Description	Risk
10.10.10.16			**Scanning...**	
			Scan Complete	
Details			Open Ports Found: 12	
53	TCP	domain	Domain Name Server	Low
80	TCP	www-http	World Wide Web HTTP	Elevated
88	TCP	kerberos	Kerberos	Low
135	TCP	loc-srv	Location Service	Low
139	TCP	netbios-ssn	NETBIOS Session Service	Elevated
389	TCP	ldap	Lightweight Directory Access Protocol	Low
445	TCP	microsoft-ds	Microsoft-DS	Low
464	TCP	kpasswd	Kerberos "passwd"	Low
636	TCP	ldaps	LDAP over SSL	Low
2103	TCP	zephyr-clt	Zephyr serv-hm connection	Low
2105	TCP	eklogin	Kerberos encrypted rlogin	Low
3389	TCP	msrdp	Microsoft Remote Display (Terminal) P...	Low

Figure 2.1.8: MegaPing Port Scanning Report

13. Similarly, you can perform port and service scanning on other target machines.

14. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.

15. Close all open windows and document all the acquired information.

TASK 2

Perform Port and Service Discovery using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

TASK 2.1

Install NetScanTools Pro

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**, and double-click **nstp11demo.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

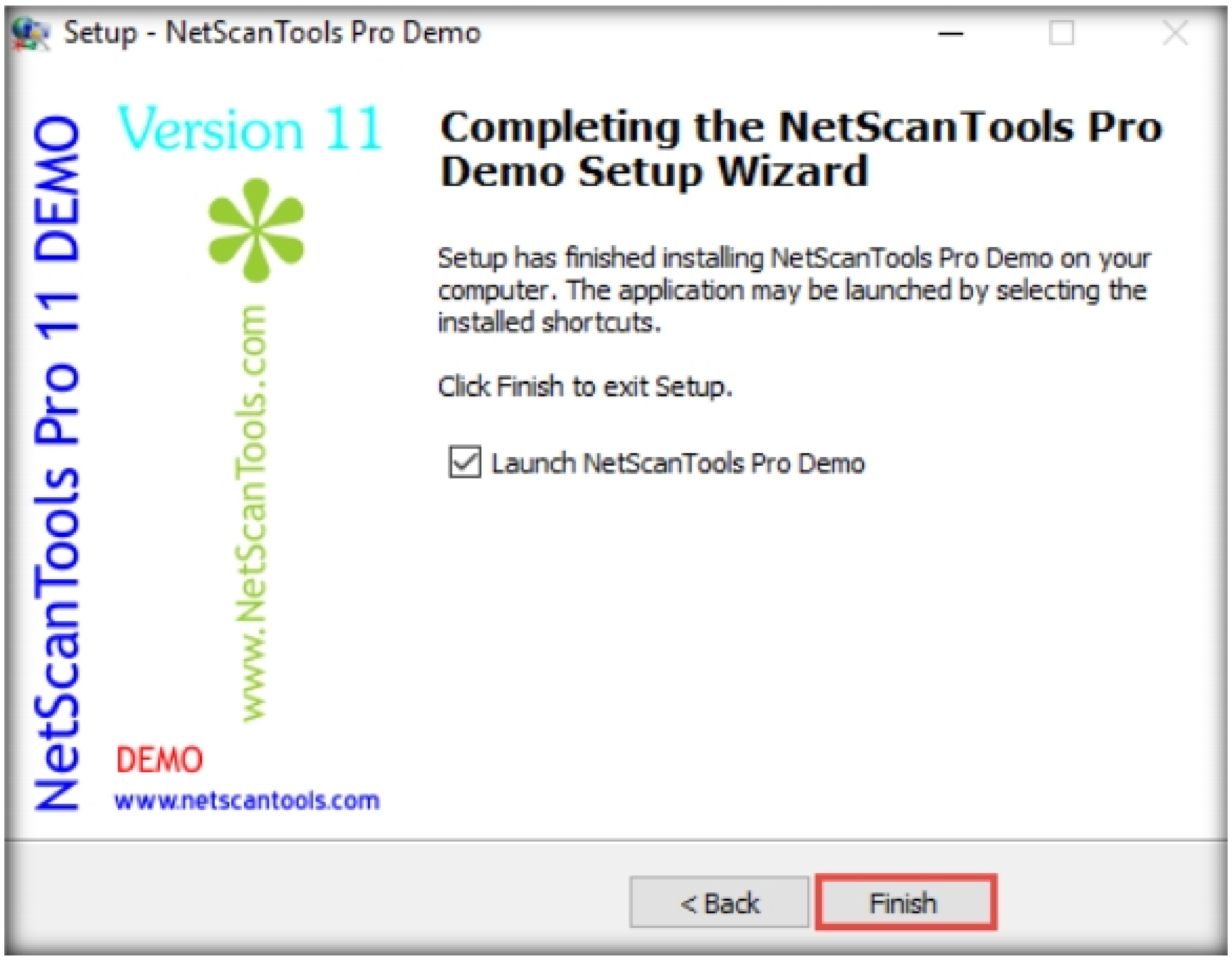
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

2. The **Setup - NetScanTools Pro Demo** window appears; click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

Note: If the **WinPcap Setup** window appears, click **Next** and install it.

3. After the completion of the installation, click **Finish**.



Completing the NetScanTools Pro Demo Setup Wizard

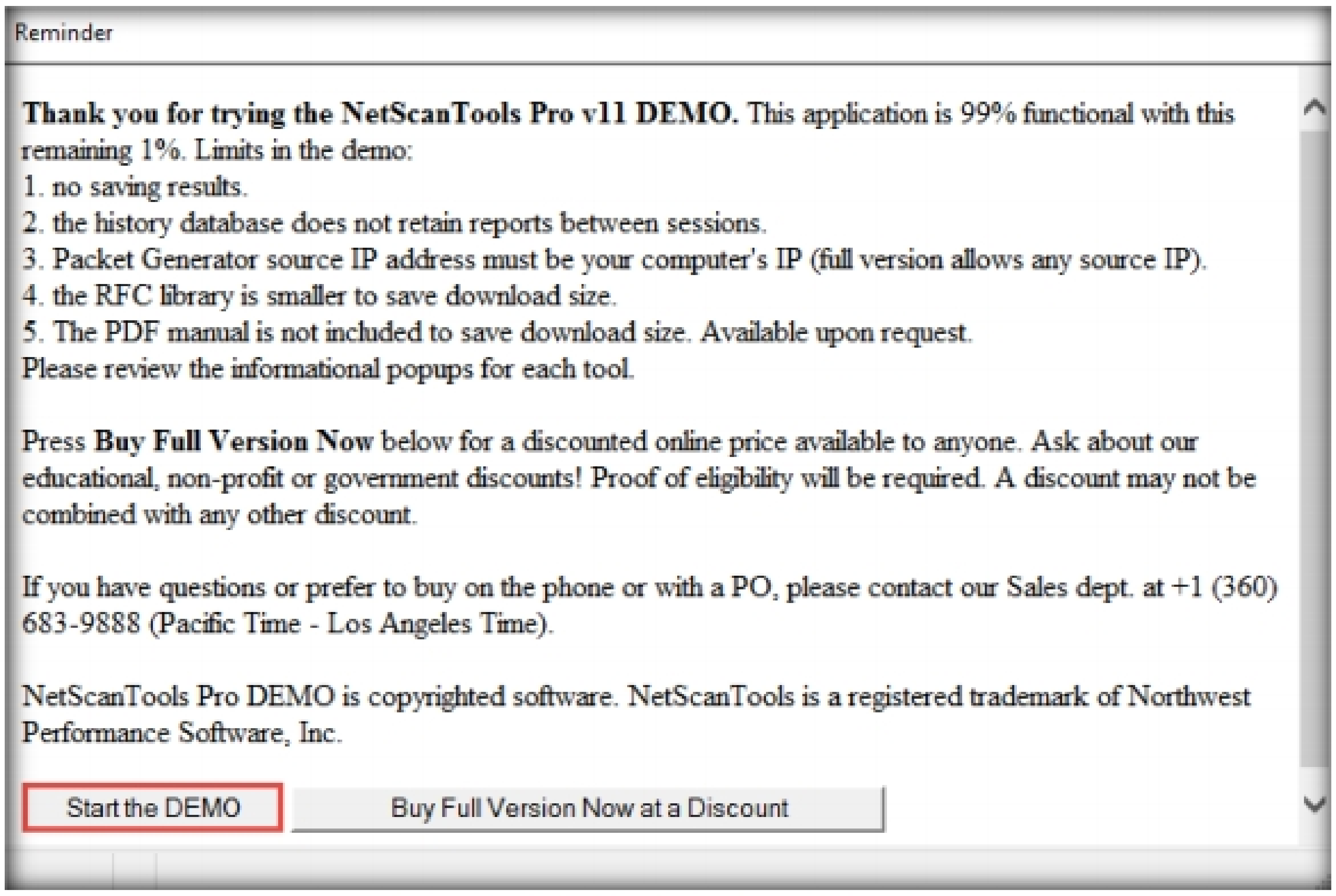
Setup has finished installing NetScanTools Pro Demo on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch NetScanTools Pro Demo

Figure 2.2.1: NetScanTools Setup window

4. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



Thank you for trying the NetScanTools Pro v11 DEMO. This application is 99% functional with this remaining 1%. Limits in the demo:
1. no saving results.
2. the history database does not retain reports between sessions.
3. Packet Generator source IP address must be your computer's IP (full version allows any source IP).
4. the RFC library is smaller to save download size.
5. The PDF manual is not included to save download size. Available upon request.
Please review the informational popups for each tool.

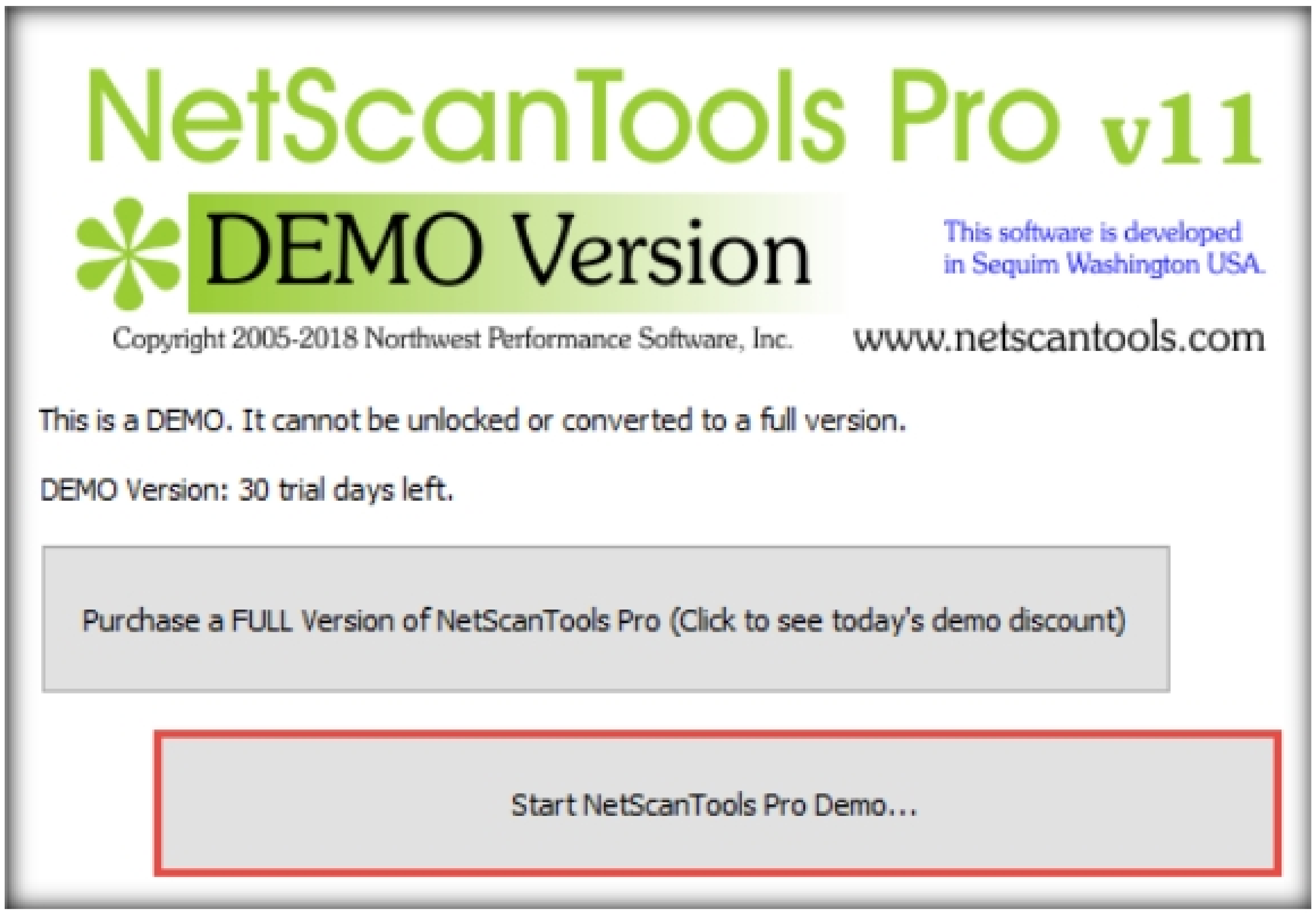
Press **Buy Full Version Now** below for a discounted online price available to anyone. Ask about our educational, non-profit or government discounts! Proof of eligibility will be required. A discount may not be combined with any other discount.

If you have questions or prefer to buy on the phone or with a PO, please contact our Sales dept. at +1 (360) 683-9888 (Pacific Time - Los Angeles Time).

NetScanTools Pro DEMO is copyrighted software. NetScanTools is a registered trademark of Northwest Performance Software, Inc.

Figure 2.2.2: NetScan Tools Pro reminder window

5. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.

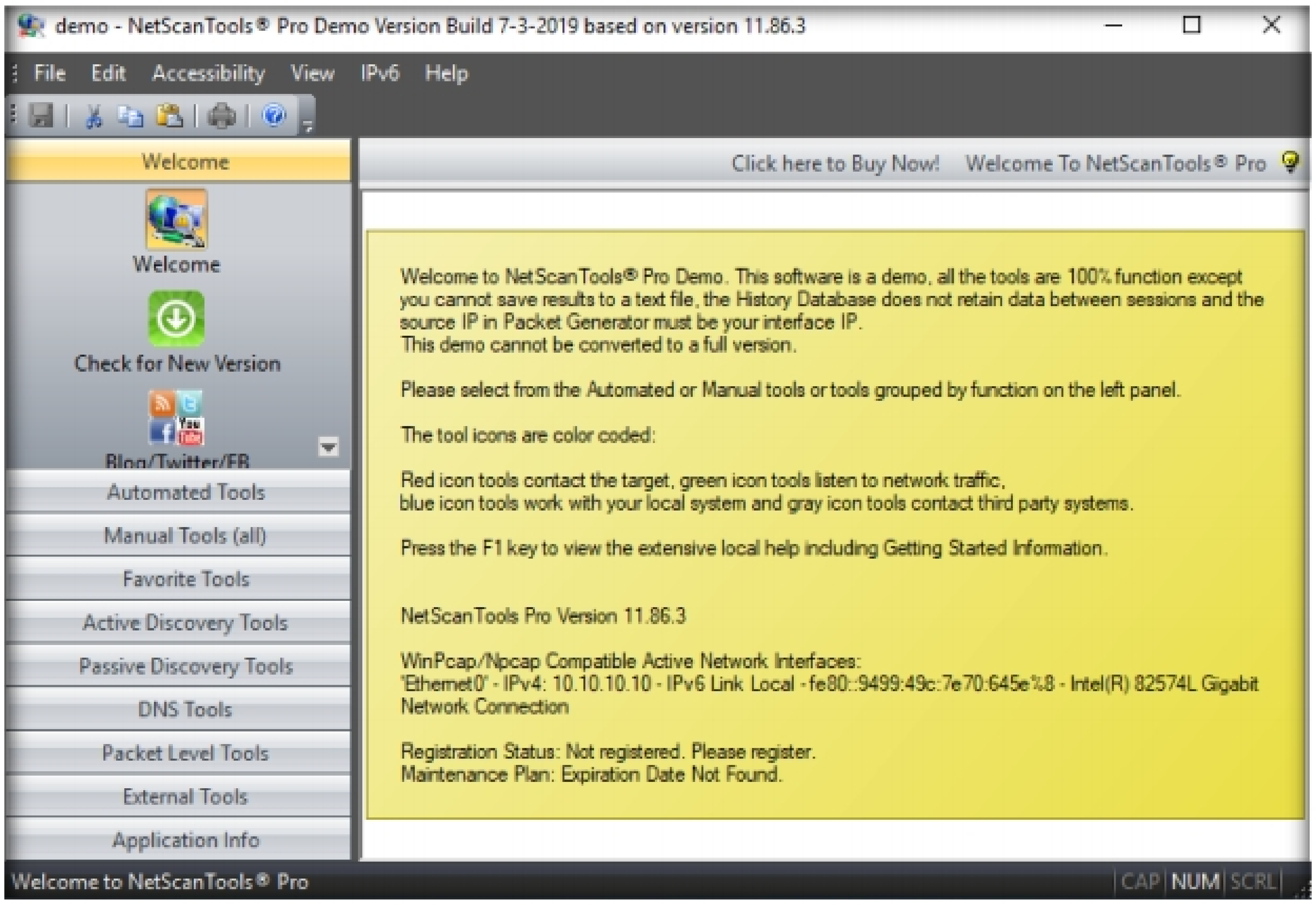

NetScanTools Pro v11
DEMO Version
This software is developed in Sequim Washington USA.
Copyright 2005-2018 Northwest Performance Software, Inc.
www.netscantools.com
Purchase a FULL Version of NetScanTools Pro (Click to see today's demo discount)
Start NetScanTools Pro Demo...

This is a DEMO. It cannot be unlocked or converted to a full version.

DEMO Version: 30 trial days left.

Figure 2.2.3: DEMO Version pop-up

6. The **NetScanTools Pro** main window appears, as shown in the screenshot.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Welcome
Check for New Version
Blog/Twitter/FB
Automated Tools
Manual Tools (all)
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Welcome To NetScanTools® Pro
Welcome to NetScanTools® Pro
CAP
NUM
SCRL

Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not retain data between sessions and the source IP in Packet Generator must be your interface IP.
This demo cannot be converted to a full version.

Please select from the Automated or Manual tools or tools grouped by function on the left panel.

The tool icons are color coded:

Red icon tools contact the target, green icon tools listen to network traffic,
blue icon tools work with your local system and gray icon tools contact third party systems.

Press the F1 key to view the extensive local help including Getting Started Information.

NetScanTools Pro Version 11.86.3

WinPcap/Npcap Compatible Active Network Interfaces:
'Ethernet0' - IPv4: 10.10.10.10 - IPv6 Link Local - fe80::9499:49c:7e70:645e%8 - Intel(R) 82574L Gigabit Network Connection

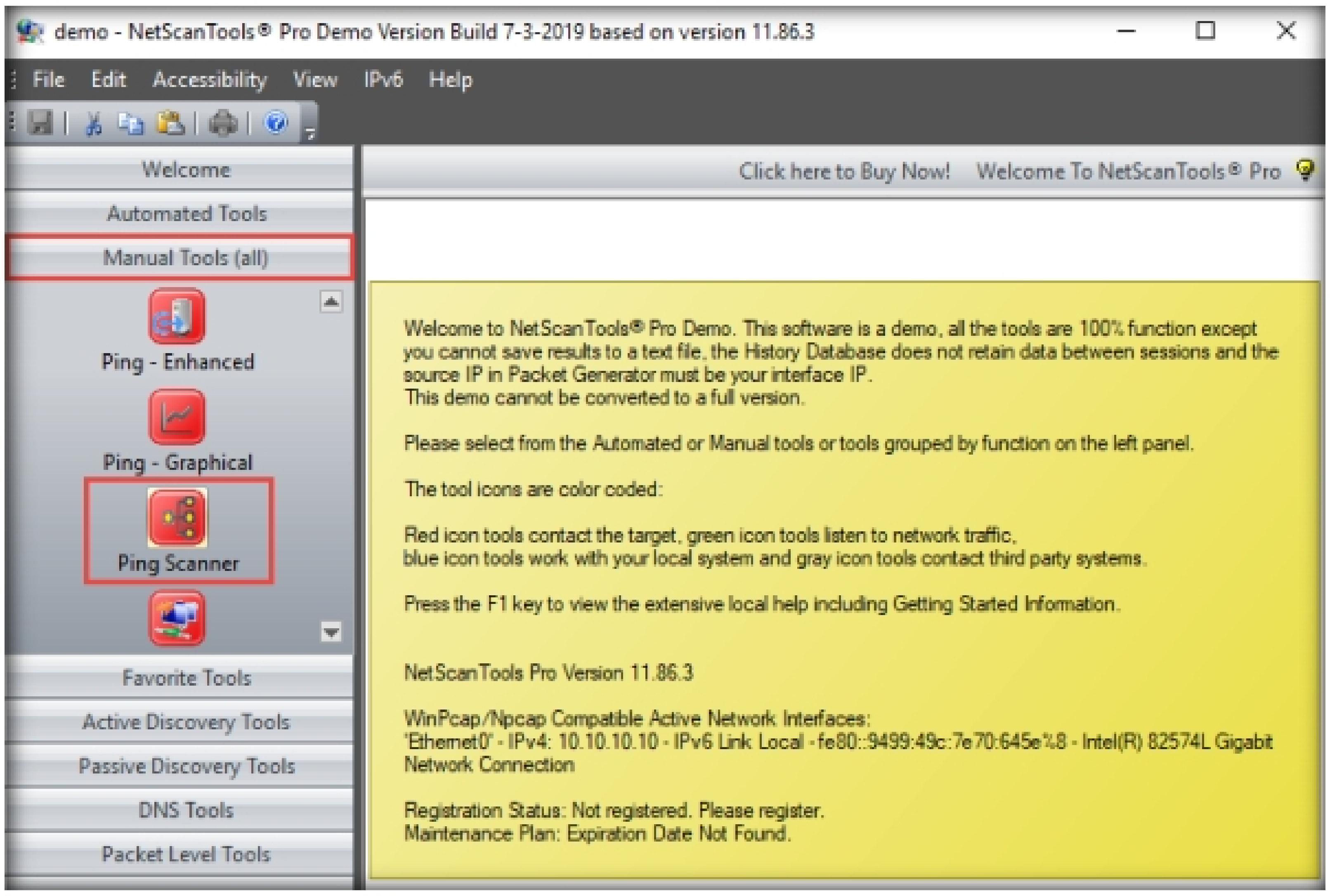
Registration Status: Not registered. Please register.
Maintenance Plan: Expiration Date Not Found.

Figure 2.2.4: Main window of NetScan Tools Pro

TASK 2.2

Perform Ping Scan

7. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Ping - Enhanced
Ping - Graphical
Ping Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
Click here to Buy Now!
Welcome To NetScanTools® Pro

Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not retain data between sessions and the source IP in Packet Generator must be your interface IP.
This demo cannot be converted to a full version.

Please select from the Automated or Manual tools or tools grouped by function on the left panel.

The tool icons are color coded:

Red icon tools contact the target, green icon tools listen to network traffic,
blue icon tools work with your local system and gray icon tools contact third party systems.

Press the F1 key to view the extensive local help including Getting Started Information.

NetScanTools Pro Version 11.86.3

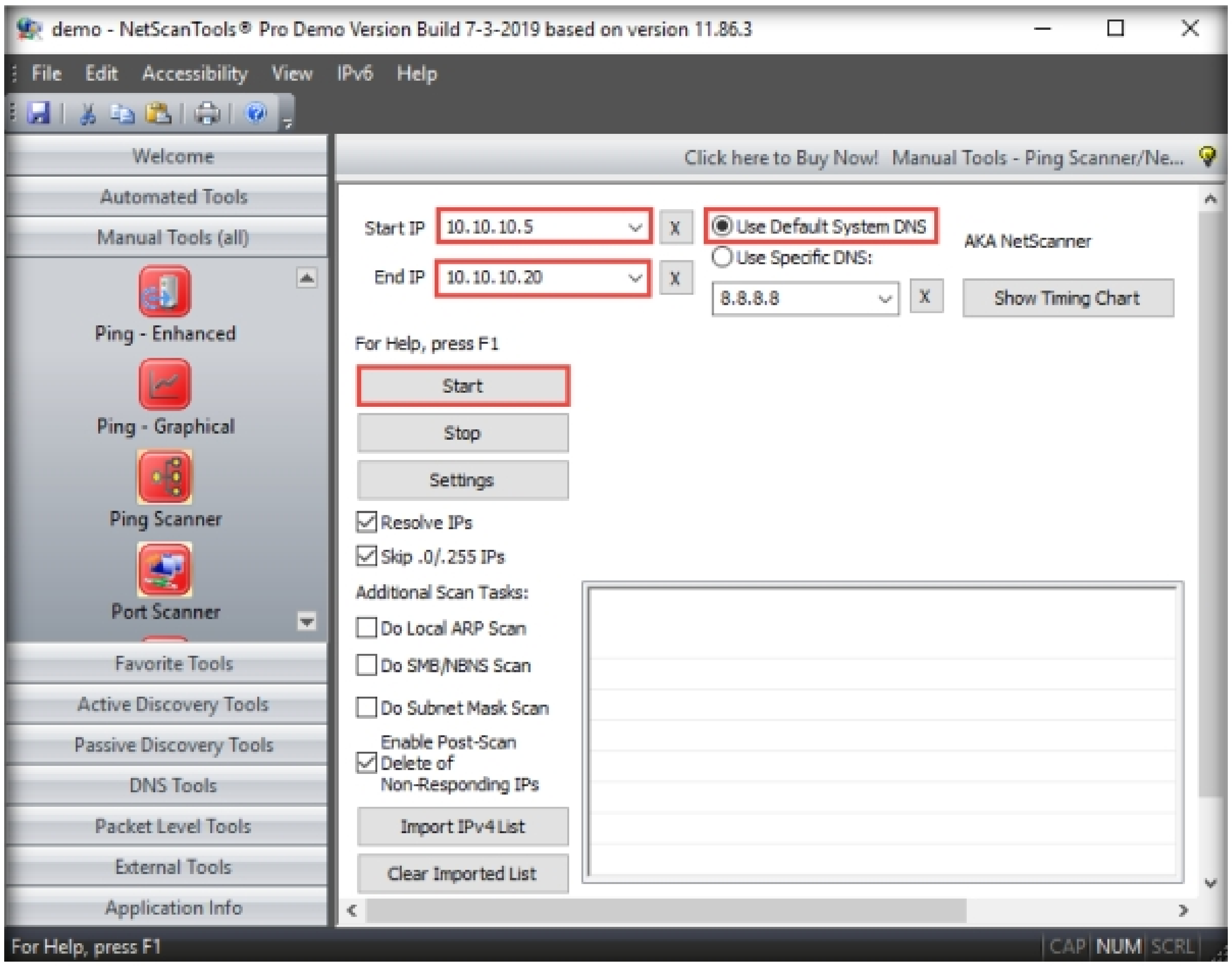
WinPcap/Npcap Compatible Active Network Interfaces:
'Ethernet0' - IPv4: 10.10.10.10 - IPv6 Link Local - fe80::9499:49c:7e70:645e%8 - Intel(R) 82574L Gigabit Network Connection

Registration Status: Not registered. Please register.
Maintenance Plan: Expiration Date Not Found.

Figure 2.2.5: Selecting Ping Scanner option

8. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.
9. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.10.5 - 10.10.10.20**); then, click **Start**.

Note: The IP address range might differ in your lab environment.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Ping - Enhanced
Ping - Graphical
Ping Scanner
Port Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - Ping Scanner/Ne...
AKA NetScanner
Show Timing Chart
For Help, press F1
Start
Stop
Settings
Import IPv4 List
Clear Imported List
X
CAP
NUM
SCRL

Start IP 10.10.10.5
End IP 10.10.10.20
● Use Default System DNS
○ Use Specific DNS: 8.8.8.8
☑ Resolve IPs
☑ Skip .0/.255 IPs
Additional Scan Tasks:
☐ Do Local ARP Scan
☐ Do SMB/NBNS Scan
☐ Do Subnet Mask Scan
☑ Enable Post-Scan Delete of Non-Responding IPs

Figure 2.2.6: Configuring the Ping Scanner tool

10. A **Ping Scanner** notice pop-up appears; click **I Accept**.

11. After the completion of the scan, if a **How do you want to open this file?** pop-up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

Note: If the browser opens automatically, skip to the next step.

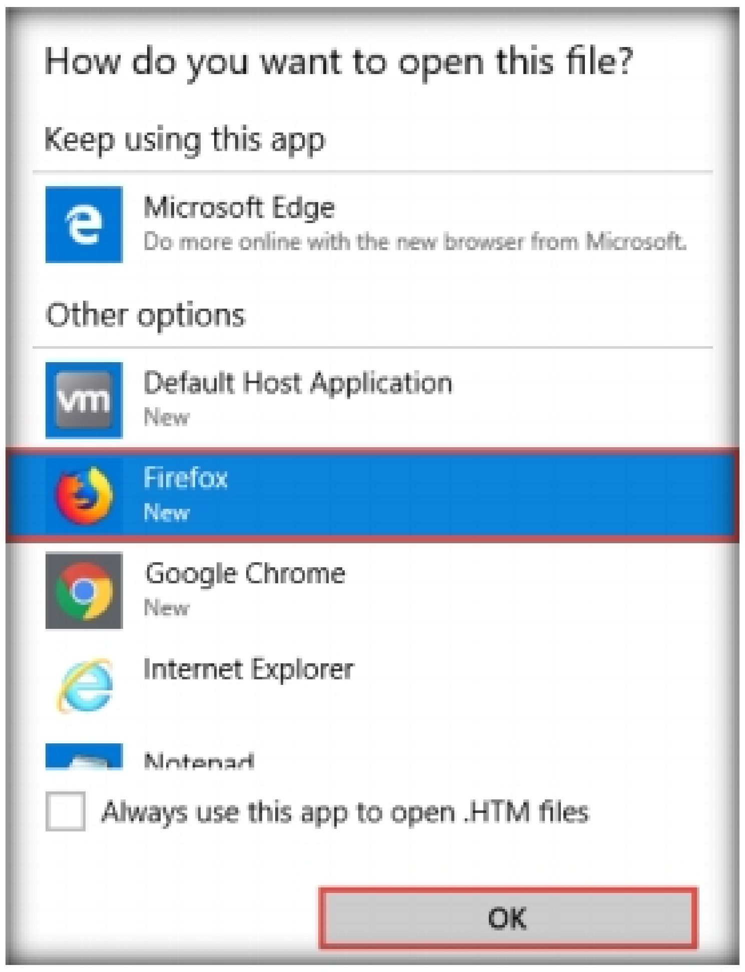
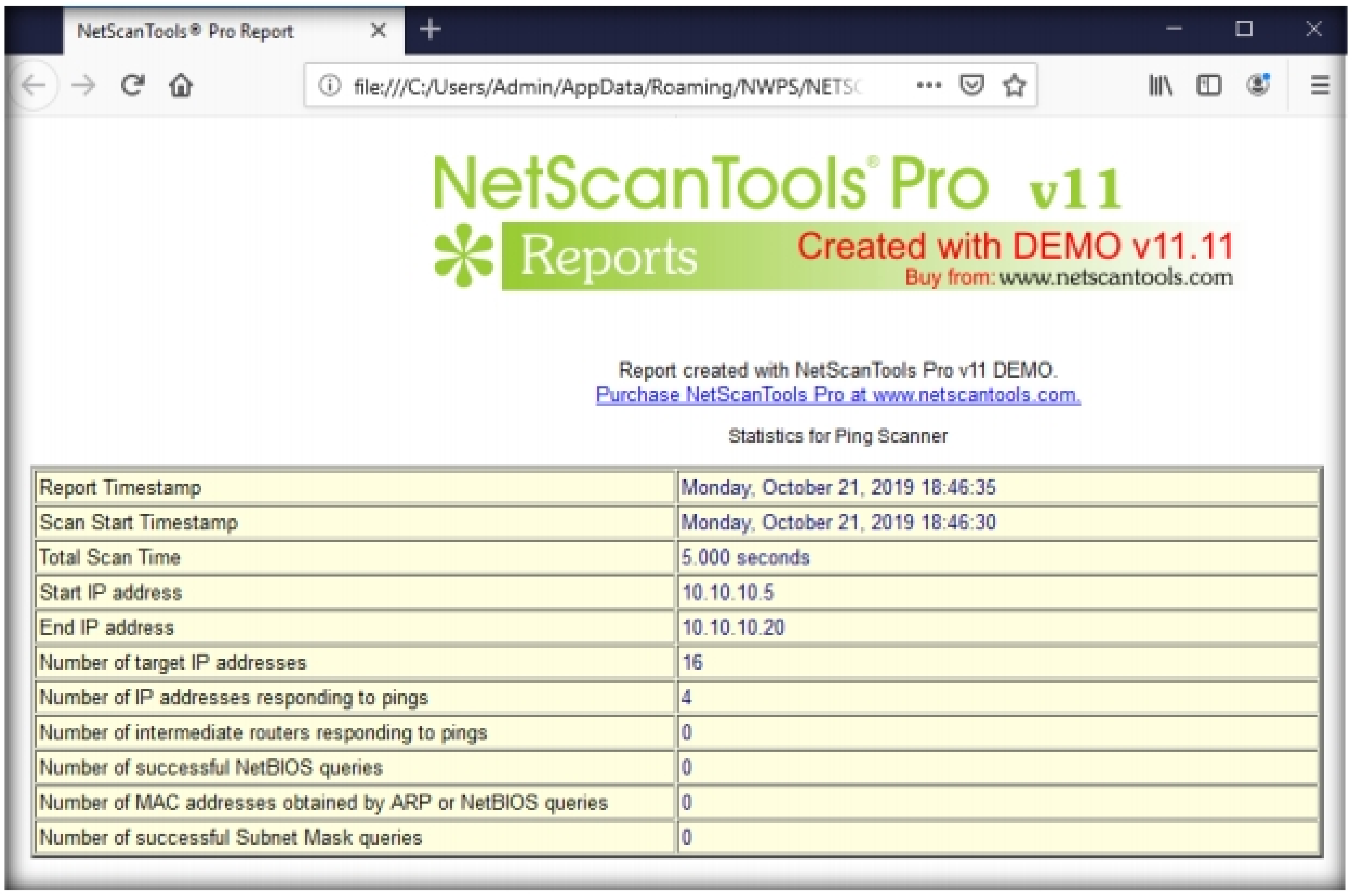

How do you want to open this file?
Keep using this app
Microsoft Edge
Do more online with the new browser from Microsoft.
Other options
Default Host Application
New
Firefox
New
Google Chrome
New
Internet Explorer
Notepad
☐ Always use this app to open .HTM files
OK

Figure 2.2.7: Choosing a browser to open the HTM file

12. A report appears in the browser displaying values such as **Start IP address**, **End IP address**, **Number of target IP addresses**, **Number of IP addresses responding to pings**, etc.

Note: The results might vary in your lab environment.


NetScanTools® Pro Report
file:///C:/Users/Admin/AppData/Roaming/NWPS/NETS
NetScanTools® Pro v11
Reports
Created with DEMO v11.11
Buy from: www.netscantools.com

Report created with NetScanTools Pro v11 DEMO.
Purchase NetScanTools Pro at www.netscantools.com.

Statistics for Ping Scanner

Report Timestamp	Monday, October 21, 2019 18:46:35
Scan Start Timestamp	Monday, October 21, 2019 18:46:30
Total Scan Time	5.000 seconds
Start IP address	10.10.10.5
End IP address	10.10.10.20
Number of target IP addresses	16
Number of IP addresses responding to pings	4
Number of intermediate routers responding to pings	0
Number of successful NetBIOS queries	0
Number of MAC addresses obtained by ARP or NetBIOS queries	0
Number of successful Subnet Mask queries	0

Figure 2.2.8: Browser displaying the scan report

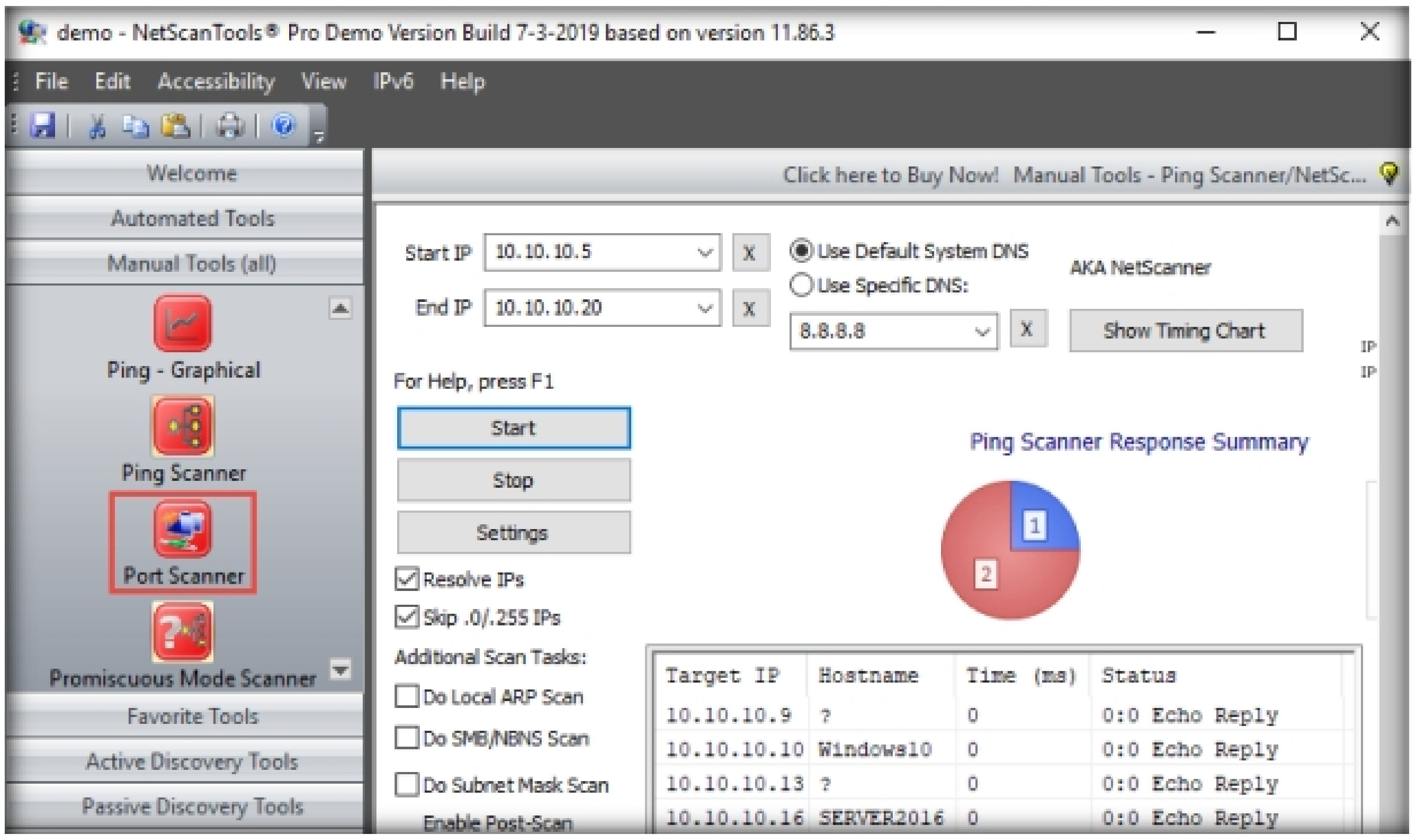
13. Close the browser and switch to the **NetScanTools Pro** window.

TASK 2.3

Perform Port Scan

14. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

Note: If a dialog box appears explaining the **Port Scanner** tool, click **OK**.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Ping - Graphical
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
Click here to Buy Now!
Manual Tools - Ping Scanner/NetSc...
AKA NetScanner
Show Timing Chart
For Help, press F1
Start
Stop
Settings
Additional Scan Tasks:
Enable Post-Scan
Ping Scanner Response Summary
1
2

Start IP: 10.10.10.5

End IP: 10.10.10.20

● Use Default System DNS

○ Use Specific DNS: 8.8.8.8

☑ Resolve IPs

☑ Skip .0/.255 IPs

☐ Do Local ARP Scan

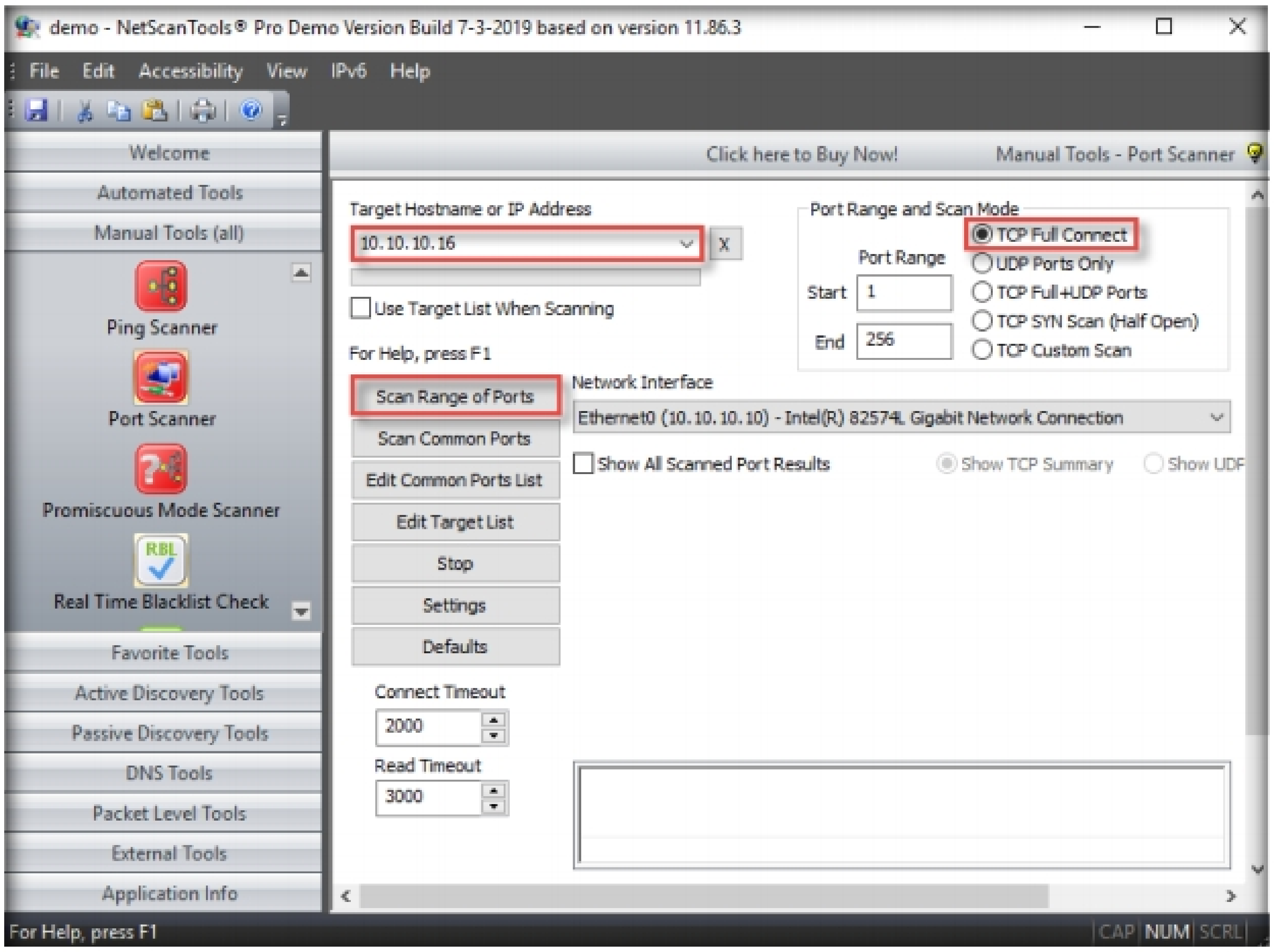
☐ Do SMB/NBNS Scan

☐ Do Subnet Mask Scan

Target IP	Hostname	Time (ms)	Status
10.10.10.9	?	0	0:0 Echo Reply
10.10.10.10	Windows10	0	0:0 Echo Reply
10.10.10.13	?	0	0:0 Echo Reply
10.10.10.16	SERVER2016	0	0:0 Echo Reply

Figure 2.2.9: Selecting Port scanner option

15. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.10.16**). Ensure that **TCP Full Connect** is selected, and then click the **Scan Range of Ports** button.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
Real Time Blacklist Check
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - Port Scanner
For Help, press F1
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
For Help, press F1
CAP
NUM
SCRL

Target Hostname or IP Address: 10.10.10.16

☐ Use Target List When Scanning

Port Range and Scan Mode

Port Range Start: 1

End: 256

● TCP Full Connect

○ UDP Ports Only

○ TCP Full+UDP Ports

○ TCP SYN Scan (Half Open)

○ TCP Custom Scan

Network Interface: Ethernet0 (10.10.10.10) - Intel(R) 82574L Gigabit Network Connection

☐ Show All Scanned Port Results

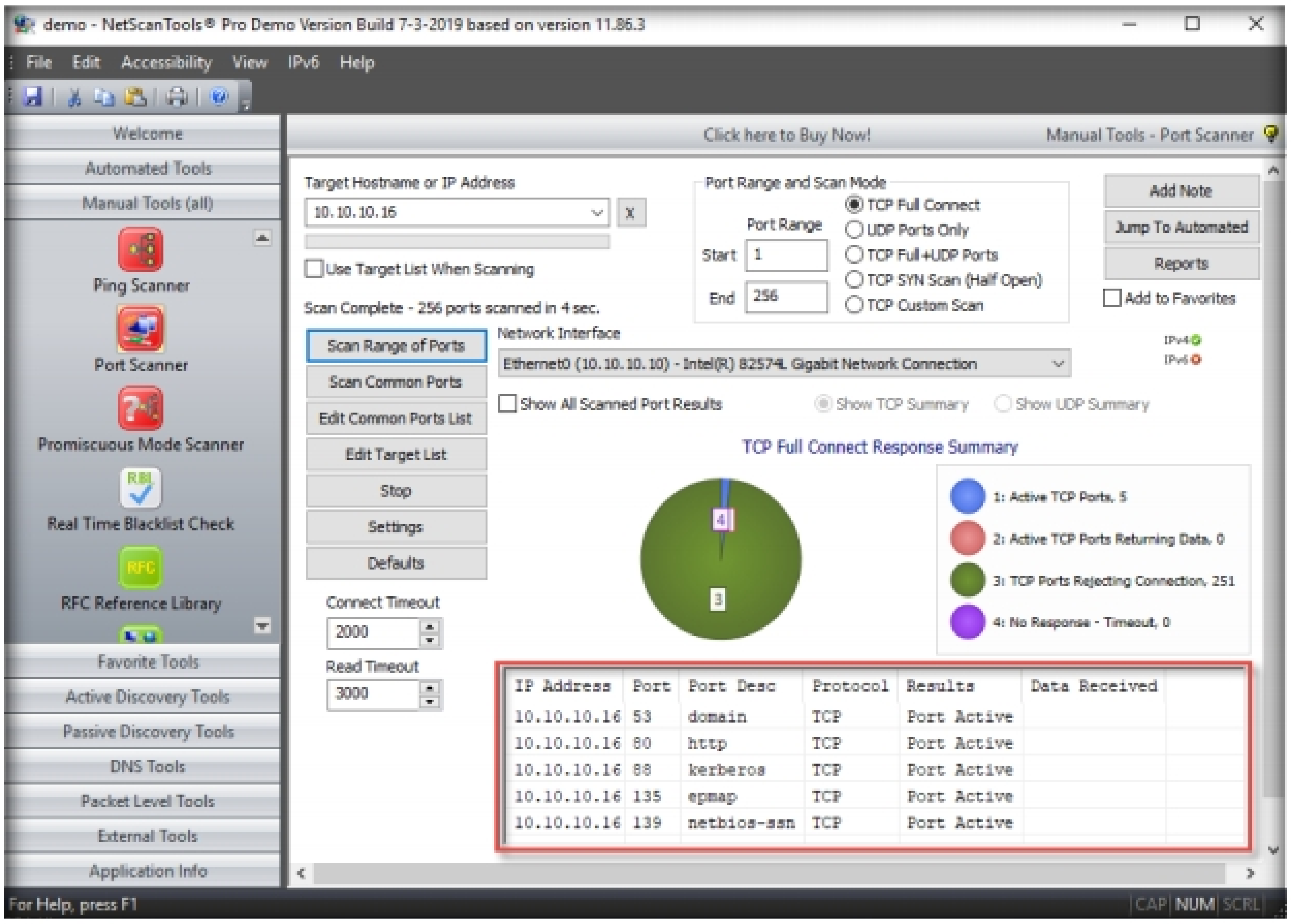
● Show TCP Summary ○ Show UDP

Connect Timeout: 2000

Read Timeout: 3000

Figure 2.2.10: Configuring the Port Scanner tool

16. A **Port Scanner** notice pop-up appears; click **I Accept**.
17. A result appears displaying the active ports and their descriptions, as shown in the screenshot.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
Real Time Blacklist Check
RFC Reference Library
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - Port Scanner
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Add Note
Jump To Automated
Reports
IPv4
IPv6
TCP Full Connect Response Summary
4
3
For Help, press F1
CAP NUM SCRL

Target Hostname or IP Address: 10.10.10.16

☐ Use Target List When Scanning

Scan Complete - 256 ports scanned in 4 sec.

Port Range and Scan Mode
Port Range Start: 1
End: 256
● TCP Full Connect
○ UDP Ports Only
○ TCP Full+UDP Ports
○ TCP SYN Scan (Half Open)
○ TCP Custom Scan

☐ Add to Favorites

Network Interface: Ethernet0 (10.10.10.10) - Intel(R) 82574L Gigabit Network Connection

☐ Show All Scanned Port Results ● Show TCP Summary ○ Show UDP Summary

Connect Timeout: 2000

Read Timeout: 3000

1: Active TCP Ports, 5
2: Active TCP Ports Returning Data, 0
3: TCP Ports Rejecting Connection, 251
4: No Response - Timeout, 0

IP Address	Port	Port Desc	Protocol	Results	Data Received
10.10.10.16	53	domain	TCP	Port Active	
10.10.10.16	80	http	TCP	Port Active	
10.10.10.16	88	kerberos	TCP	Port Active	
10.10.10.16	135	epmap	TCP	Port Active	
10.10.10.16	139	netbios-ssn	TCP	Port Active	

Figure 2.2.11: Port Scanner result

Note: By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.

18. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
19. Close all open windows and document all the acquired information.
20. Turn off the **Parrot Security** and **Ubuntu** virtual machines.

TASK 3

Explore Various Network Scanning Techniques using Nmap

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Before beginning this lab task, ensure that the **Windows Server 2016** virtual machine is turned on.

Note: In this lab task, we are using **Windows Server 2016** as a target machine.

2. In the **Windows 10** virtual machine, click on the **Start** menu and launch the **Nmap - Zenmap GUI** from the applications.

TASK 3.1

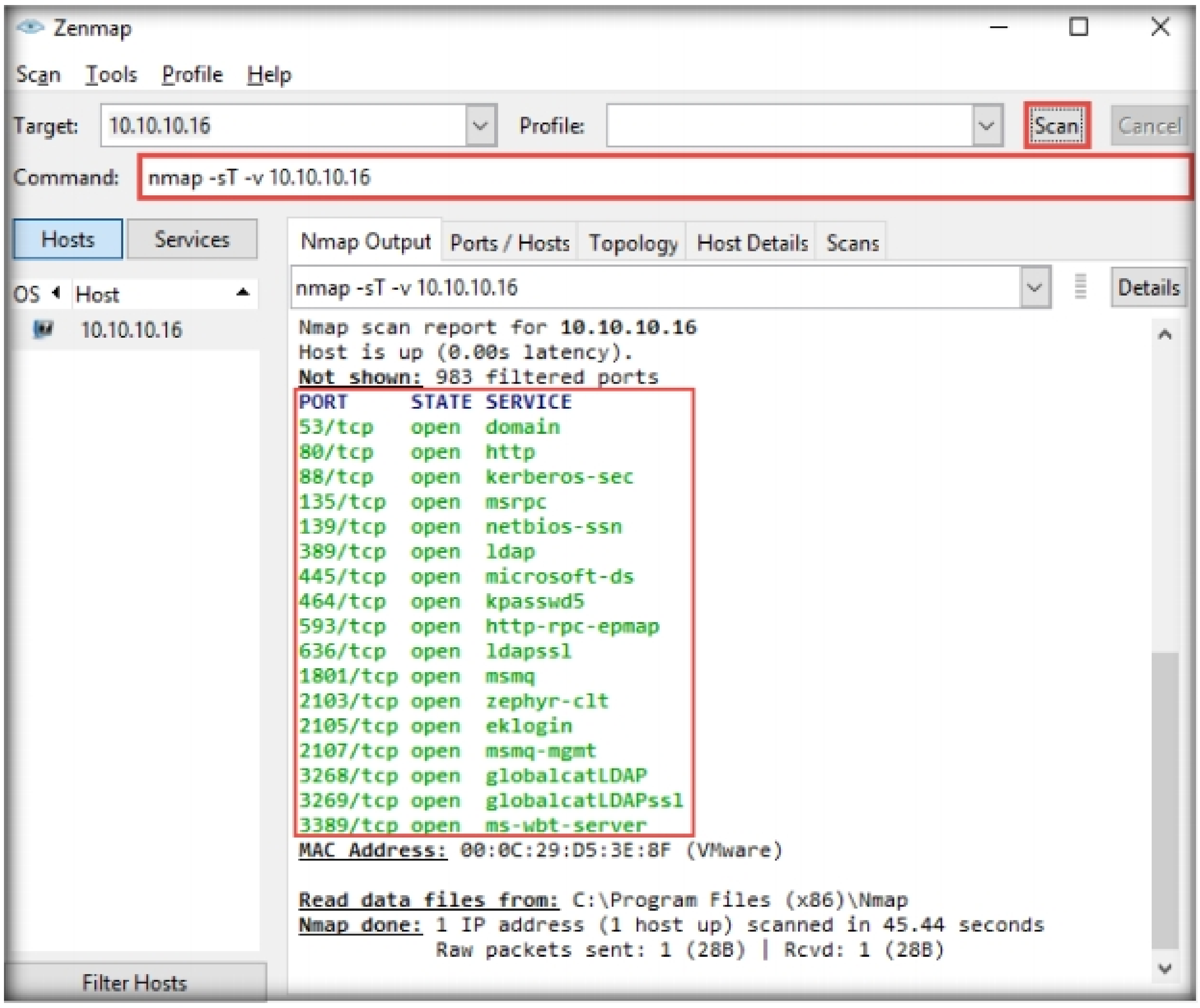
Perform TCP Connect/Full Open Scan

3. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sT -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sT**: performs the TCP connect/full open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

4. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.



Target: 10.10.10.16

Command: nmap -sT -v 10.10.10.16

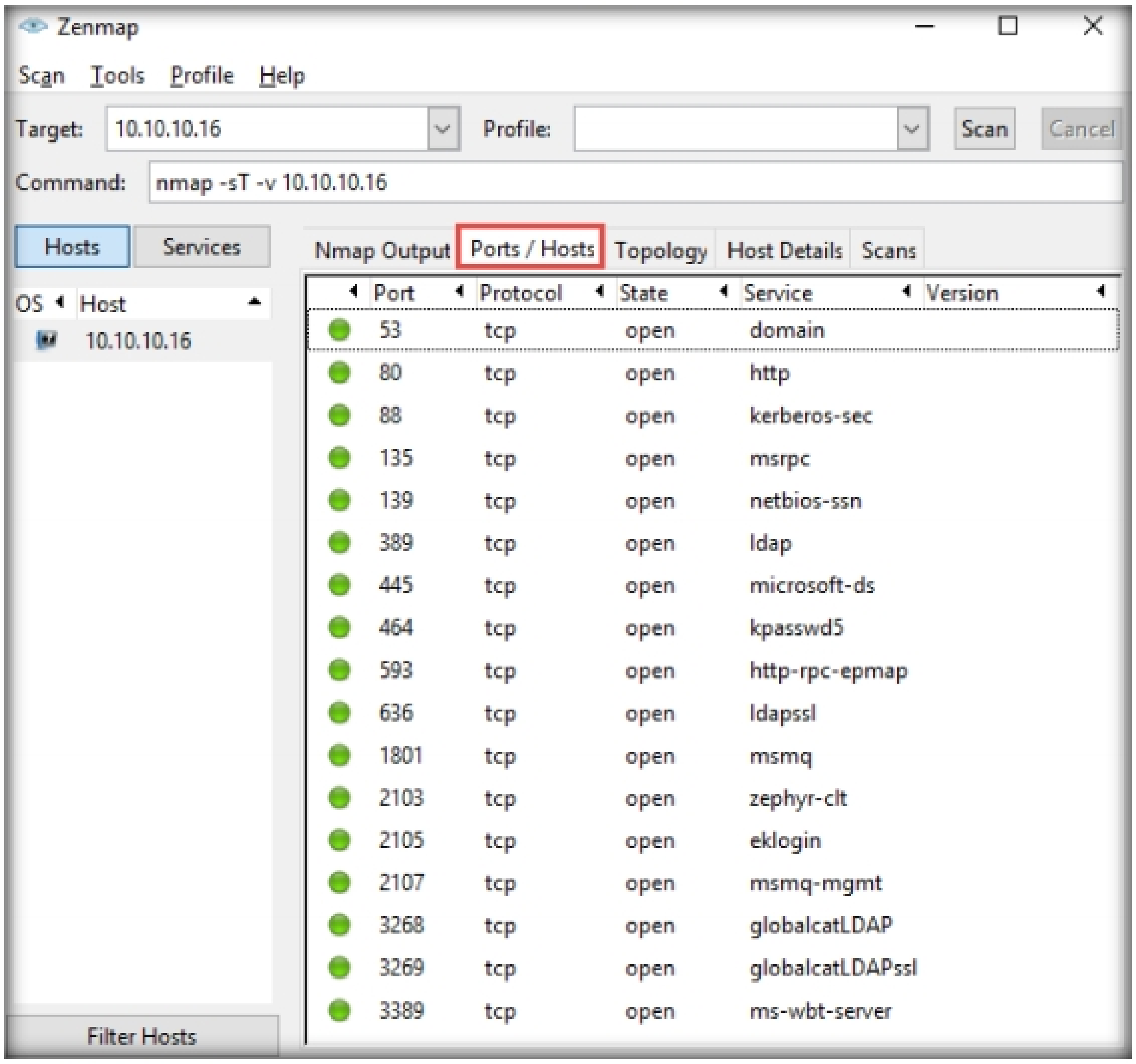
10.10.10.16

```
nmap -sT -v 10.10.10.16
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 983 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 45.44 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Figure 2.3.1: Zenmap scan results for TCP connect scan

Note: TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with the SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the client sends an RST packet to end the connection.

5. Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.


Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
10.10.10.16
Filter Hosts

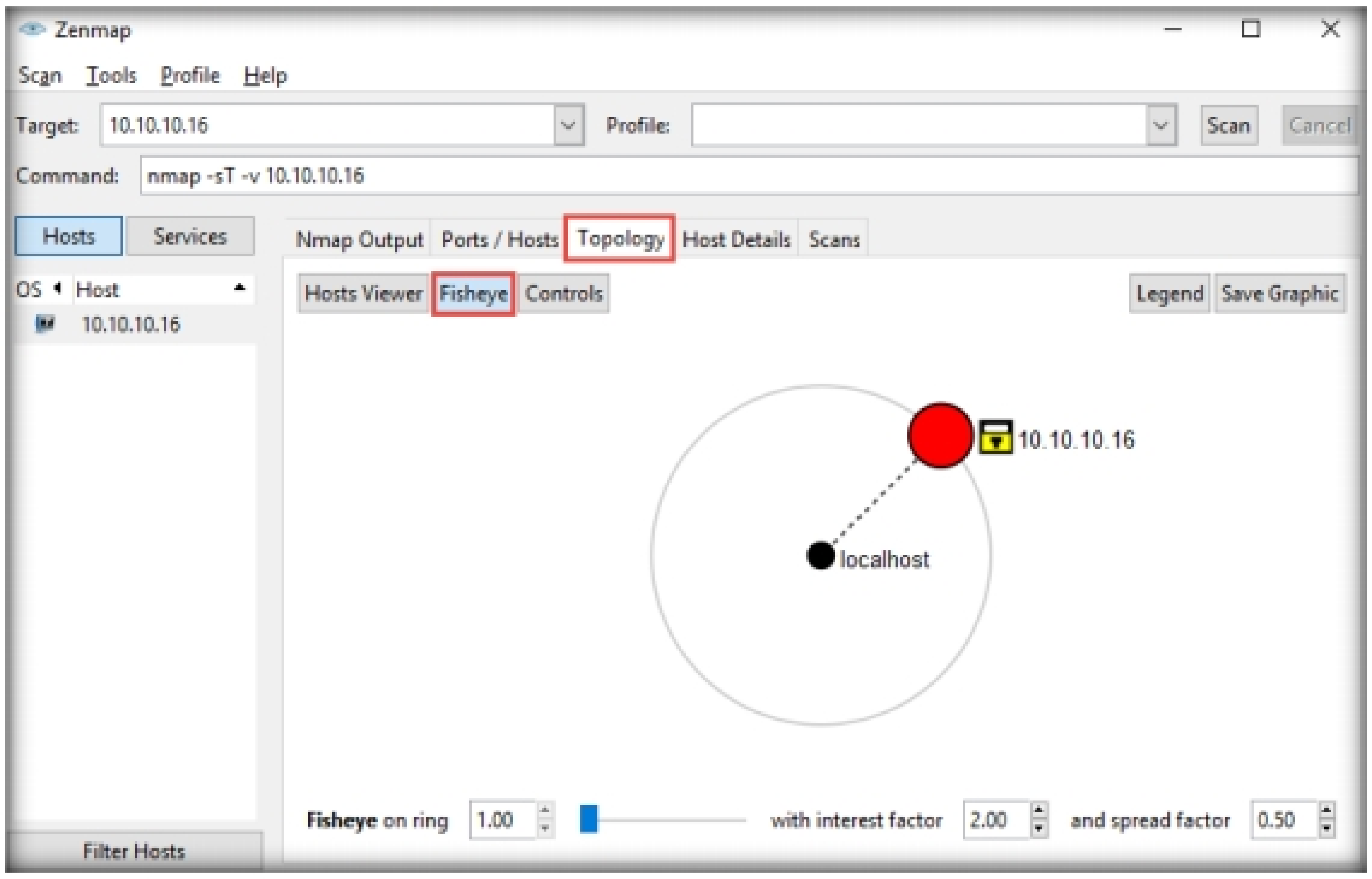
Target: 10.10.10.16

Command: nmap -sT -v 10.10.10.16

Port	Protocol	State	Service	Version
53	tcp	open	domain	
80	tcp	open	http	
88	tcp	open	kerberos-sec	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
445	tcp	open	microsoft-ds	
464	tcp	open	kpasswd5	
593	tcp	open	http-rpc-epmap	
636	tcp	open	ldapssl	
1801	tcp	open	msmq	
2103	tcp	open	zephyr-clt	
2105	tcp	open	eklogin	
2107	tcp	open	msmq-mgmt	
3268	tcp	open	globalcatLDAP	
3269	tcp	open	globalcatLDAPssl	
3389	tcp	open	ms-wbt-server	

Figure 2.3.2: Zenmap Ports / Hosts tab

6. Click the **Topology** tab to view the topology of the target network that contains the provided IP address and click the **Fisheye** option to view the topology clearly.


Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
OS
Host
10.10.10.16
10.10.10.16
localhost
Filter Hosts

Target: 10.10.10.16

Command: nmap -sT -v 10.10.10.16

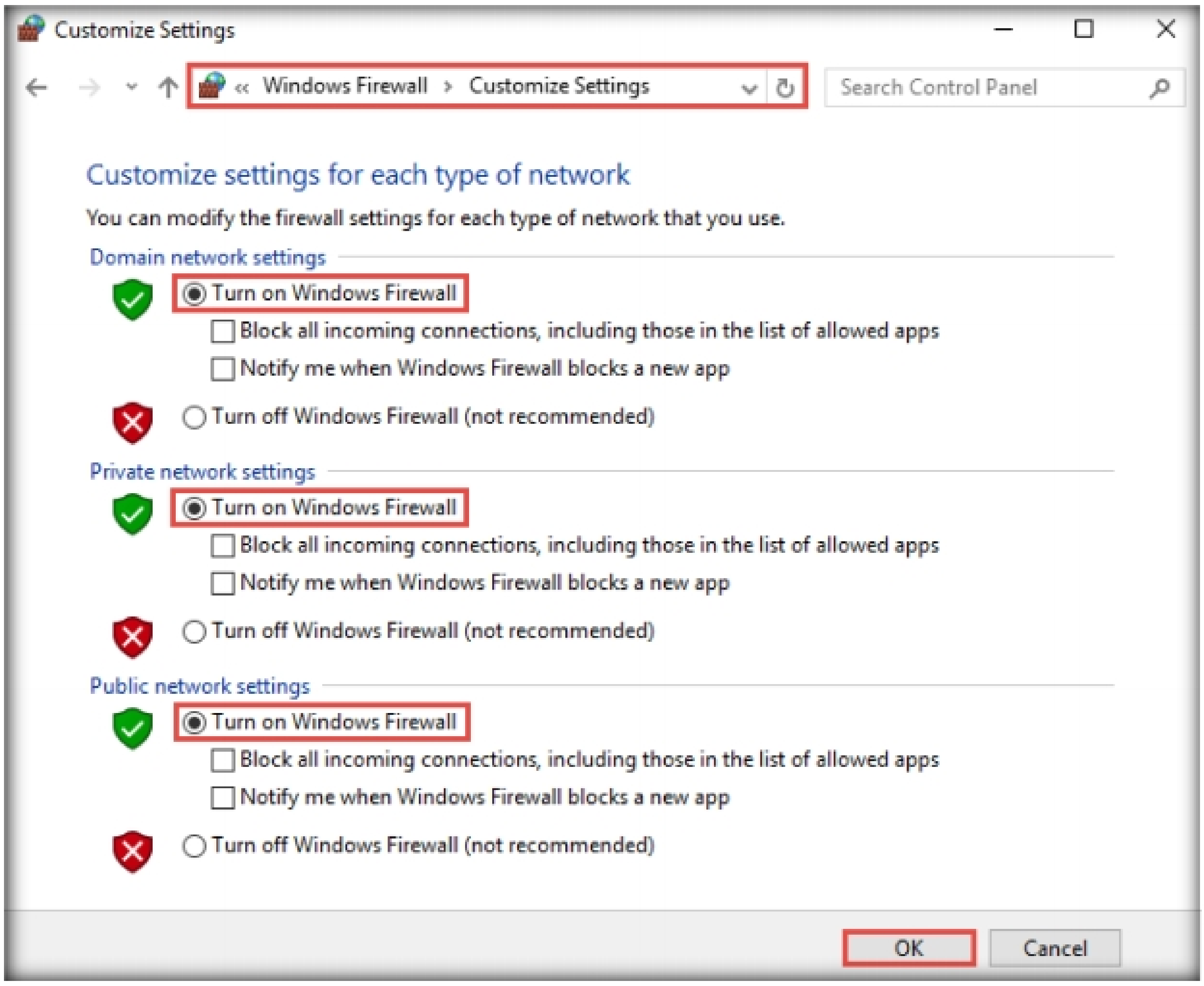
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Figure 2.3.3: Zenmap displaying topology of the selected target

7. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.
8. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.
9. Click the **Services** tab located in the right pane of the window. This tab displays a list of services.

Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

10. In this lab, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2016**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2016** virtual machine.
11. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator**/**Pa$$w0rd**.
12. Navigate to **Control Panel** → **System and Security** → **Windows Firewall** → **Turn Windows Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

● Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Private network settings

● Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Figure 2.3.4: Turn on Windows Firewall

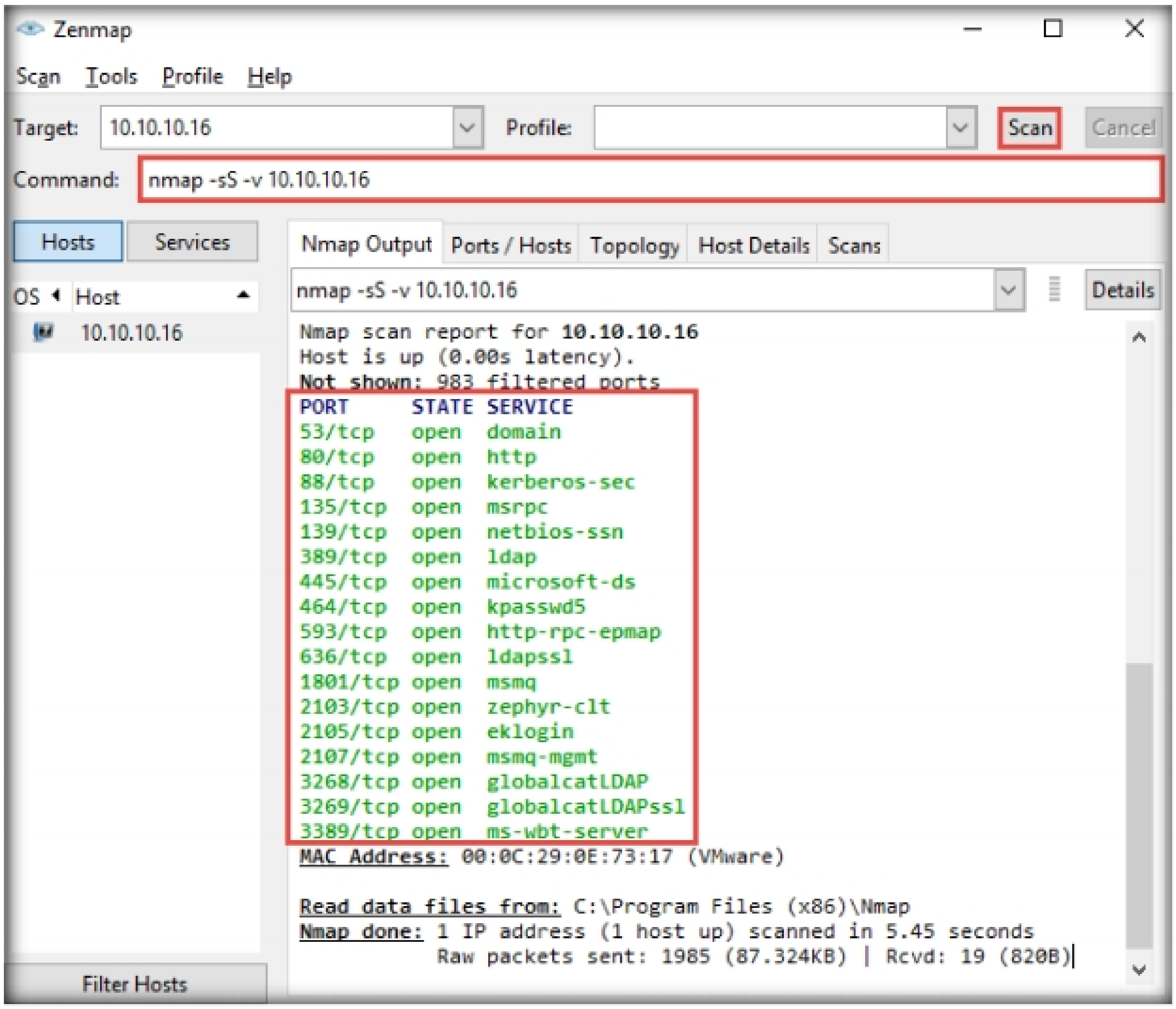
TASK 3.2

Perform Stealth Scan/TCP Half Open Scan

13. Now, switch to the **Windows 10** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sS**: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

14. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



Target: 10.10.10.16

Command: nmap -sS -v 10.10.10.16

Host: 10.10.10.16

```
nmap -sS -v 10.10.10.16
```

```
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 983 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:0E:73:17 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds
           Raw packets sent: 1985 (87.324KB) | Rcvd: 19 (820B)
```

Figure 2.3.5: Zenmap scan results for Stealth scan

Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

15. As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.

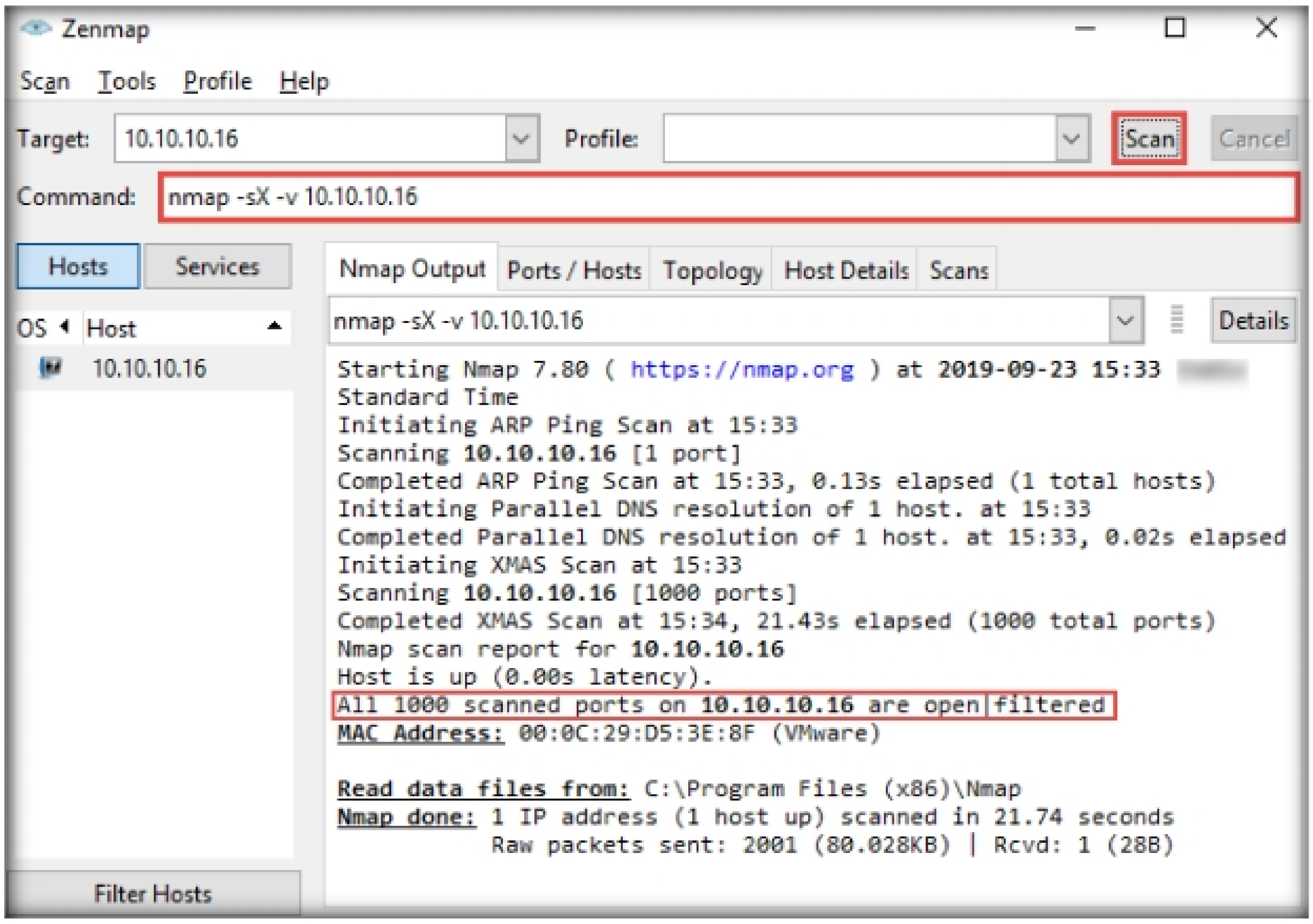
TASK 3.3

Perform Xmas Scan

16. In the **Command** field of **Zenmap**, type the command **nmap -sX -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sX**: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.



Target: 10.10.10.16

Command: nmap -sX -v 10.10.10.16

10.10.10.16

```
nmap -sX -v 10.10.10.16
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-23 15:33 [redacted]
Standard Time
Initiating ARP Ping Scan at 15:33
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 15:33, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 0.02s elapsed
Initiating XMAS Scan at 15:33
Scanning 10.10.10.16 [1000 ports]
Completed XMAS Scan at 15:34, 21.43s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.16 are open|filtered
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 21.74 seconds
           Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
```

Figure 2.3.6: Zenmap scan results for Xmas scan

Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

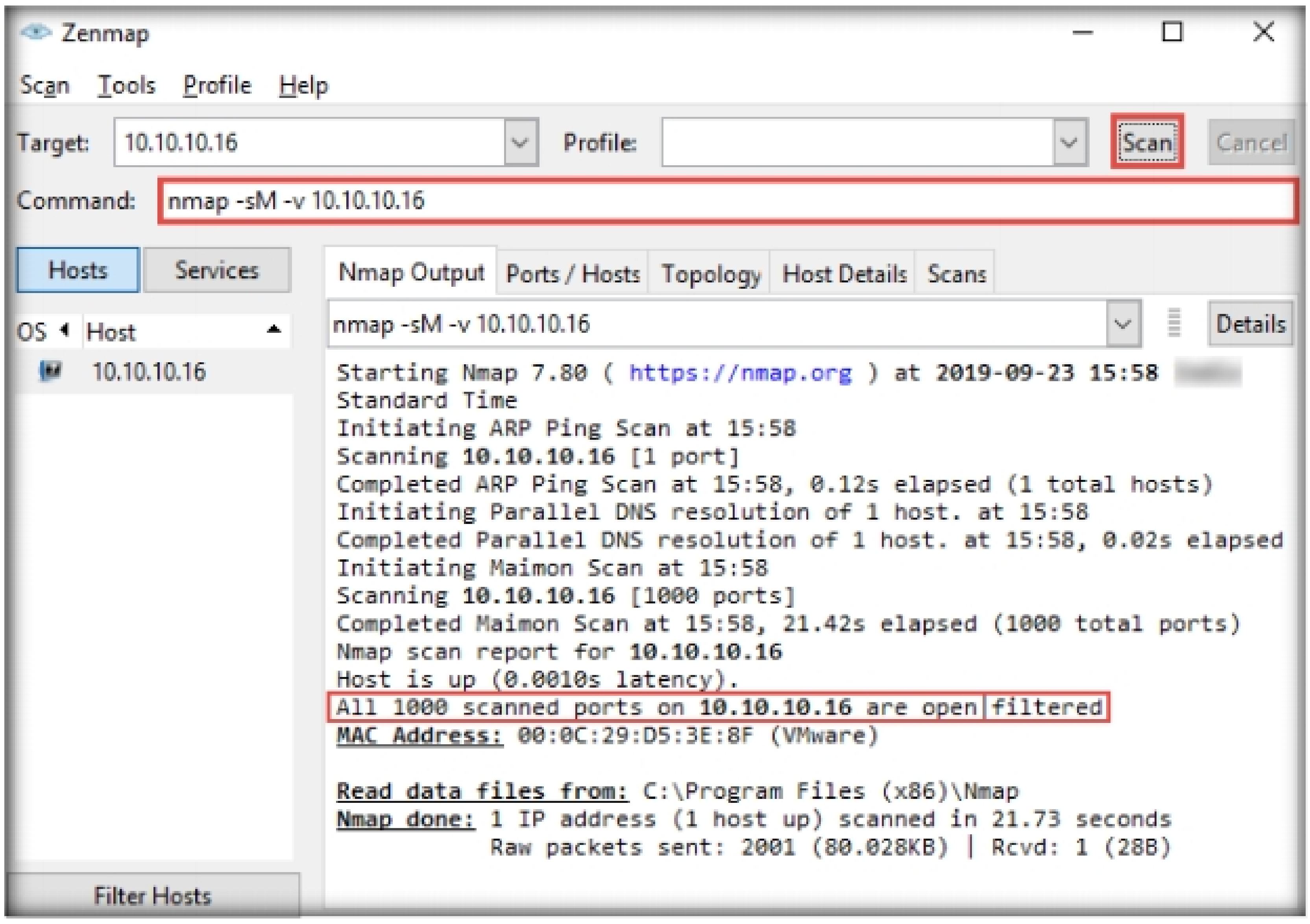
TASK 3.4

Perform TCP Maimon Scan

18. In the **Command** field, type the command **nmap -sM -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**

Note: **-sM**: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

19. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.


Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sM -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sM -v 10.10.10.16
Details
Filter Hosts

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-23 15:58 [redacted]
Standard Time
Initiating ARP Ping Scan at 15:58
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 15:58, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:58
Completed Parallel DNS resolution of 1 host. at 15:58, 0.02s elapsed
Initiating Maimon Scan at 15:58
Scanning 10.10.10.16 [1000 ports]
Completed Maimon Scan at 15:58, 21.42s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.0010s latency).
All 1000 scanned ports on 10.10.10.16 are open|filtered
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 21.73 seconds
           Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
```

Figure 2.3.7: Zenmap scan results for Stealth scan

Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.

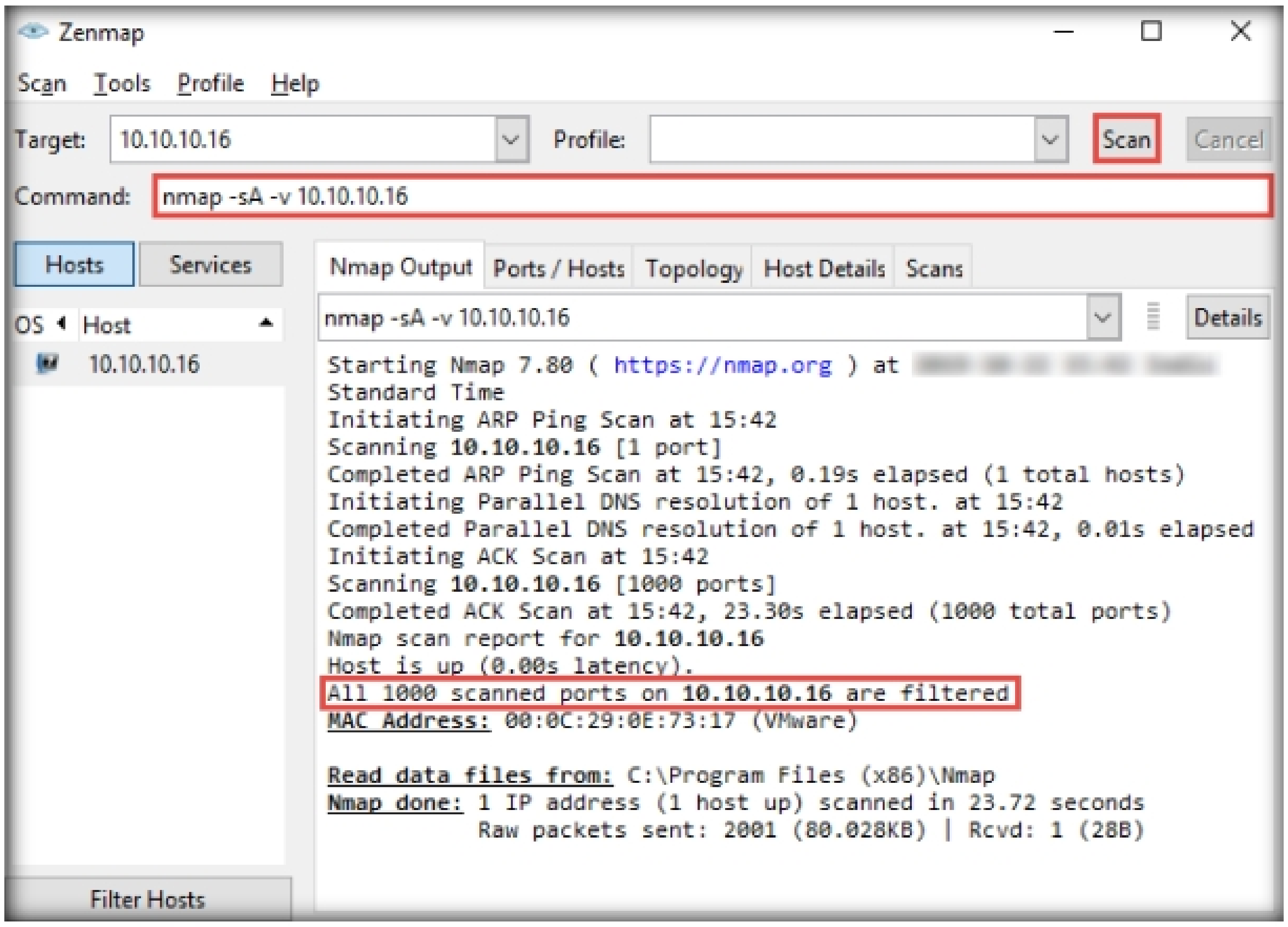
TASK 3.5

Perform ACK Flag Probe Scan

20. In the **Command** field, type the command **nmap -sA -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sA**: performs the ACK flag probe scan and **-v**: enables the verbose output (include all hosts and ports in the output).

21. The scan results appear, displaying that the ports are unfiltered on the target machine, as shown in the screenshot.

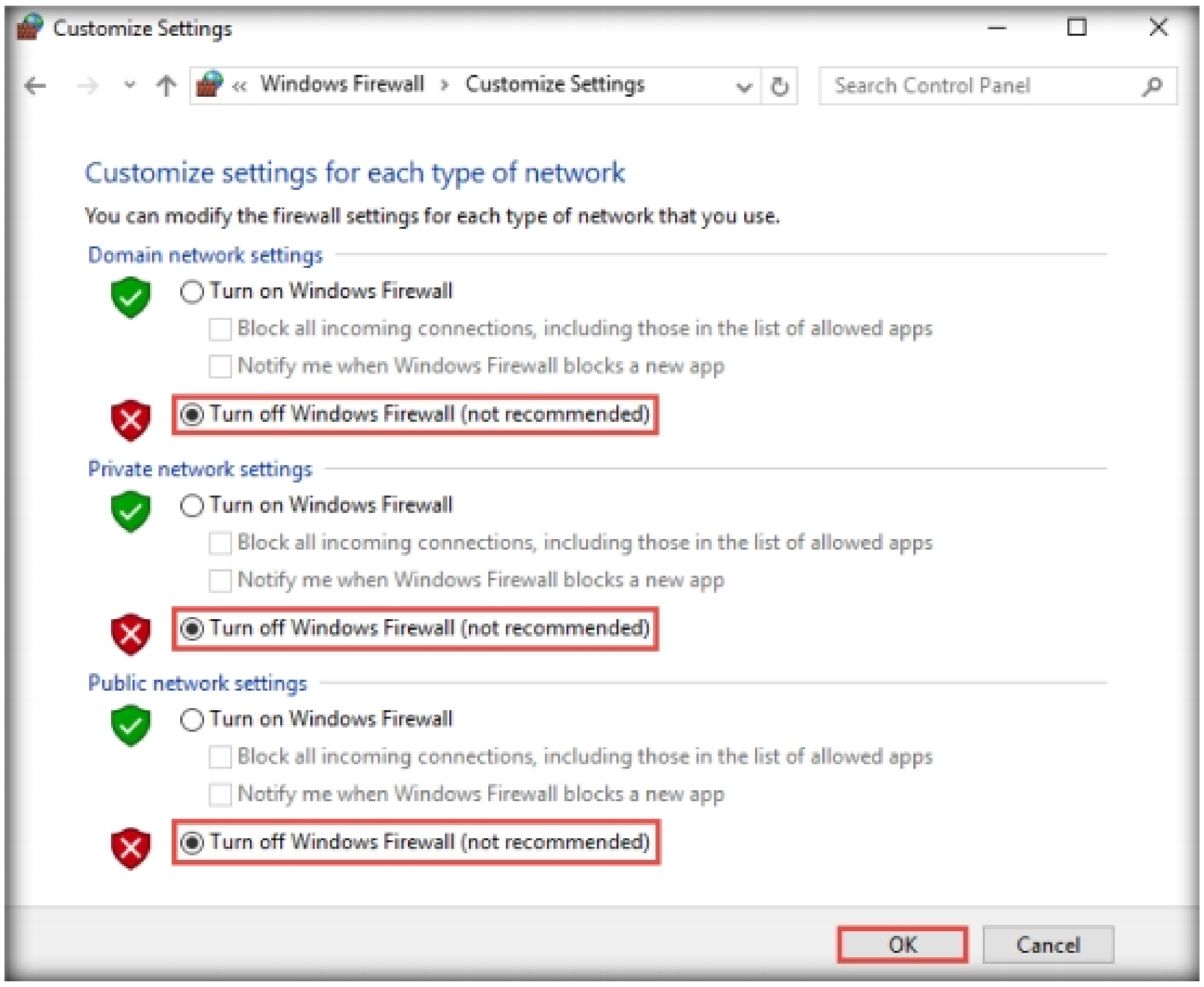

Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sA -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sA -v 10.10.10.16
Details
Filter Hosts

```
Starting Nmap 7.80 ( https://nmap.org ) at [redacted]
Standard Time
Initiating ARP Ping Scan at 15:42
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 15:42, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:42
Completed Parallel DNS resolution of 1 host. at 15:42, 0.01s elapsed
Initiating ACK Scan at 15:42
Scanning 10.10.10.16 [1000 ports]
Completed ACK Scan at 15:42, 23.30s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.16 are filtered
MAC Address: 00:0C:29:0E:73:17 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.72 seconds
           Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
```

Figure 2.3.8: Zenmap scan results for Stealth scan

Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.

22. Now, switch to the **Windows Server 2016** virtual machine and turn off the **Windows Firewall** from **Control Panel**.


Customize Settings
« Windows Firewall › Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
● Turn off Windows Firewall (not recommended)

Private network settings

○ Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall
☐ Block all incoming connections, including those in the list of allowed apps
☐ Notify me when Windows Firewall blocks a new app
● Turn off Windows Firewall (not recommended)

Figure 2.3.9: Turning off Windows Firewall

TASK 3.6

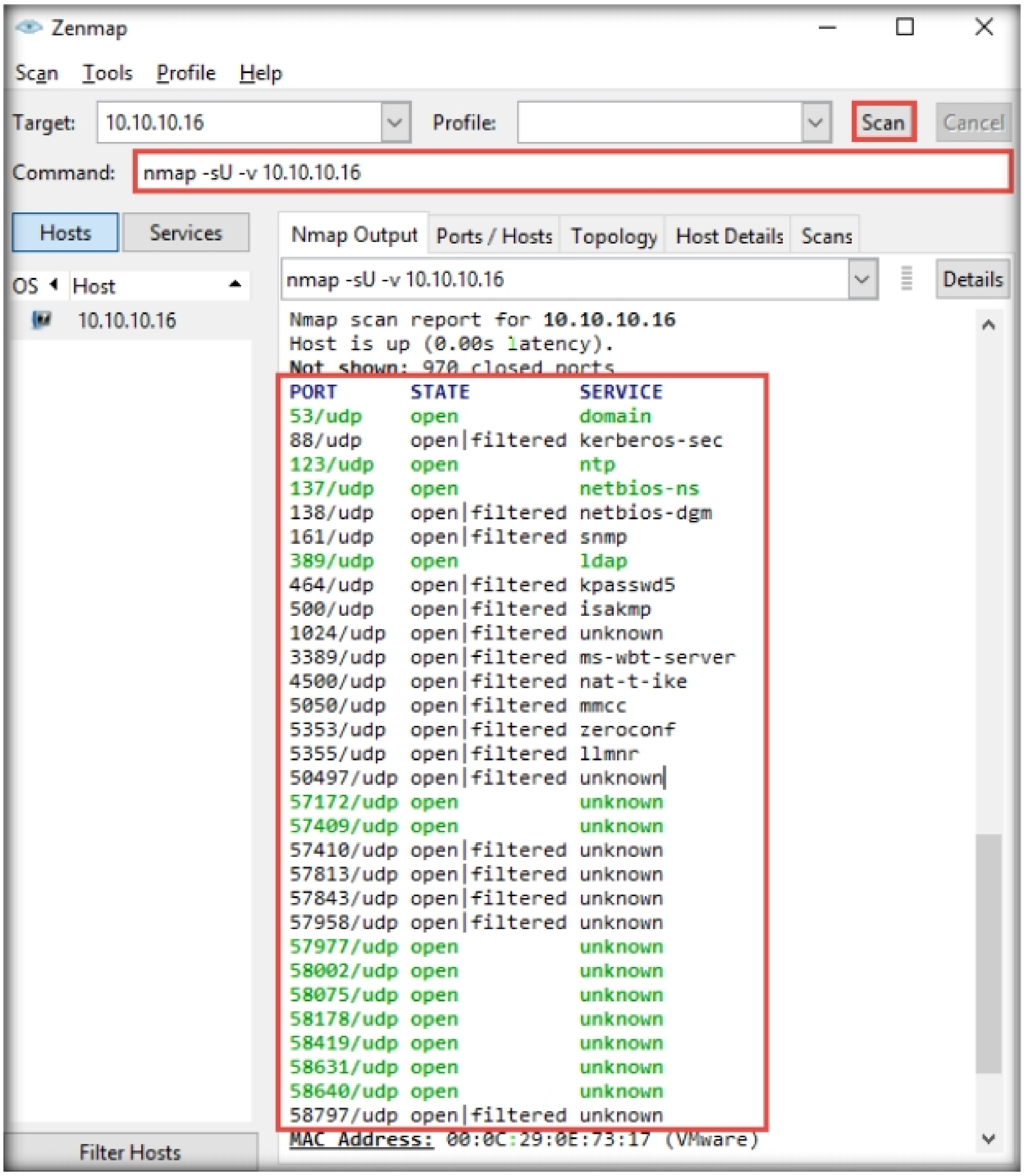
Perform UDP Scan

23. Now, return to the **Windows 10** virtual machine. In the **Command** field, type the command **nmap -sU -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU**: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output).

24. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

Note: This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.



Target: 10.10.10.16

Profile:

Command: nmap -sU -v 10.10.10.16

10.10.10.16

nmap -sU -v 10.10.10.16

```
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 970 closed ports
PORT       STATE         SERVICE
53/udp     open          domain
88/udp     open|filtered kerberos-sec
123/udp    open          ntp
137/udp    open          netbios-ns
138/udp    open|filtered netbios-dgm
161/udp    open|filtered snmp
389/udp    open          ldap
464/udp    open|filtered kpasswd5
500/udp    open|filtered isakmp
1024/udp   open|filtered unknown
3389/udp   open|filtered ms-wbt-server
4500/udp   open|filtered nat-t-ike
5050/udp   open|filtered mmcc
5353/udp   open|filtered zeroconf
5355/udp   open|filtered llmnr
50497/udp  open|filtered unknown
57172/udp  open          unknown
57409/udp  open          unknown
57410/udp  open|filtered unknown
57813/udp  open|filtered unknown
57843/udp  open|filtered unknown
57958/udp  open|filtered unknown
57977/udp  open          unknown
58002/udp  open          unknown
58075/udp  open          unknown
58178/udp  open          unknown
58419/udp  open          unknown
58631/udp  open          unknown
58640/udp  open          unknown
58797/udp  open|filtered unknown
MAC Address: 00:0C:29:0E:73:17 (VMware)
```

Figure 2.3.10: Zenmap- scan results for UDP scan

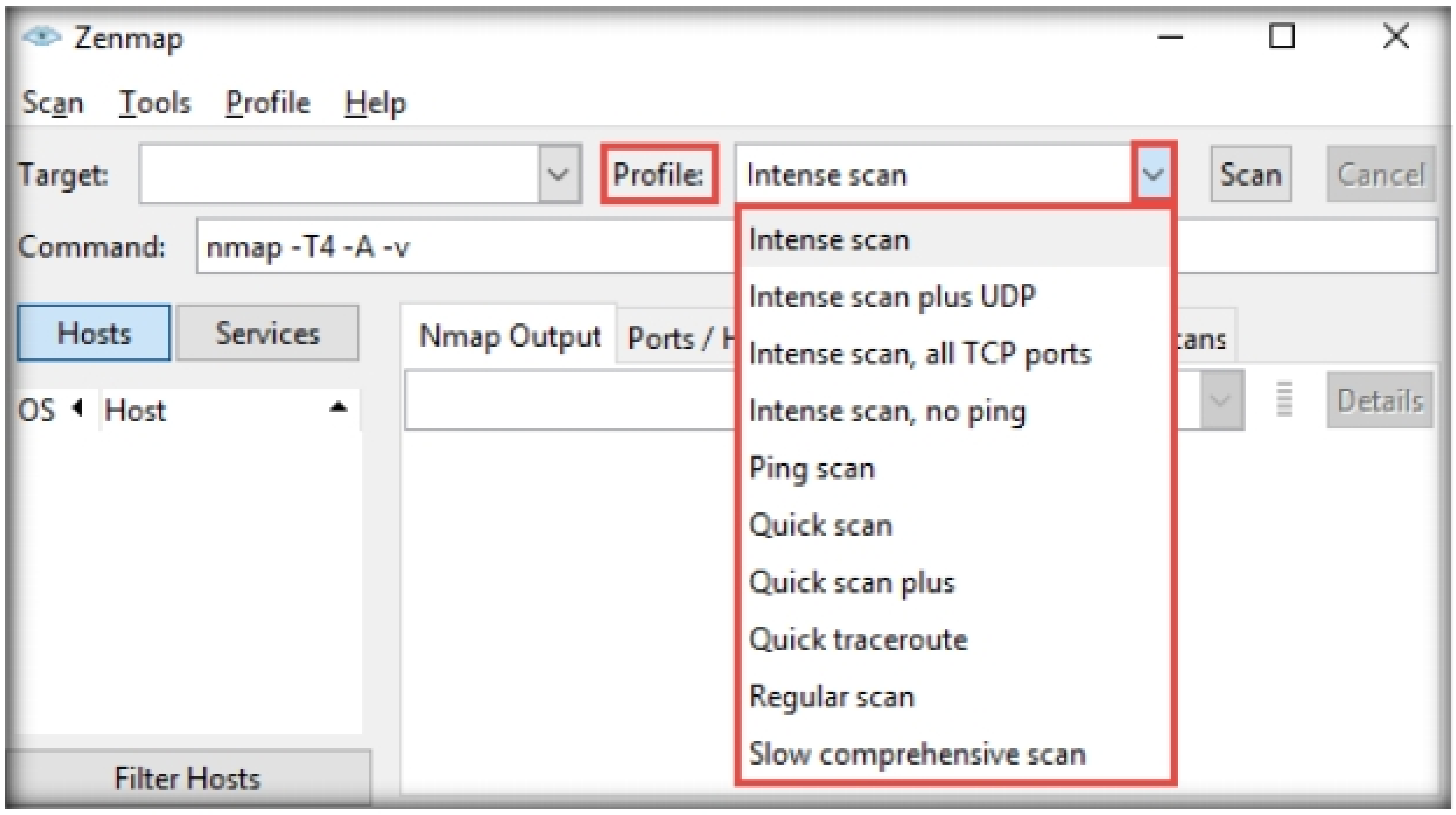
Note: The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.

25. Close the **Zenmap** window.

26. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network

27. Double-click the **Nmap - Zenmap GUI** shortcut from **Desktop** to launch Nmap.

28. To choose the default scan profiles available in Nmap, click on the drop-down icon in the **Profile** field and select the scanning technique you want to use.


Target:
Profile: Intense scan
Command: nmap -T4 -A -v

Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts
Services
Nmap Output
Ports / H
ans
OS
Host
Details
Filter Hosts
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan

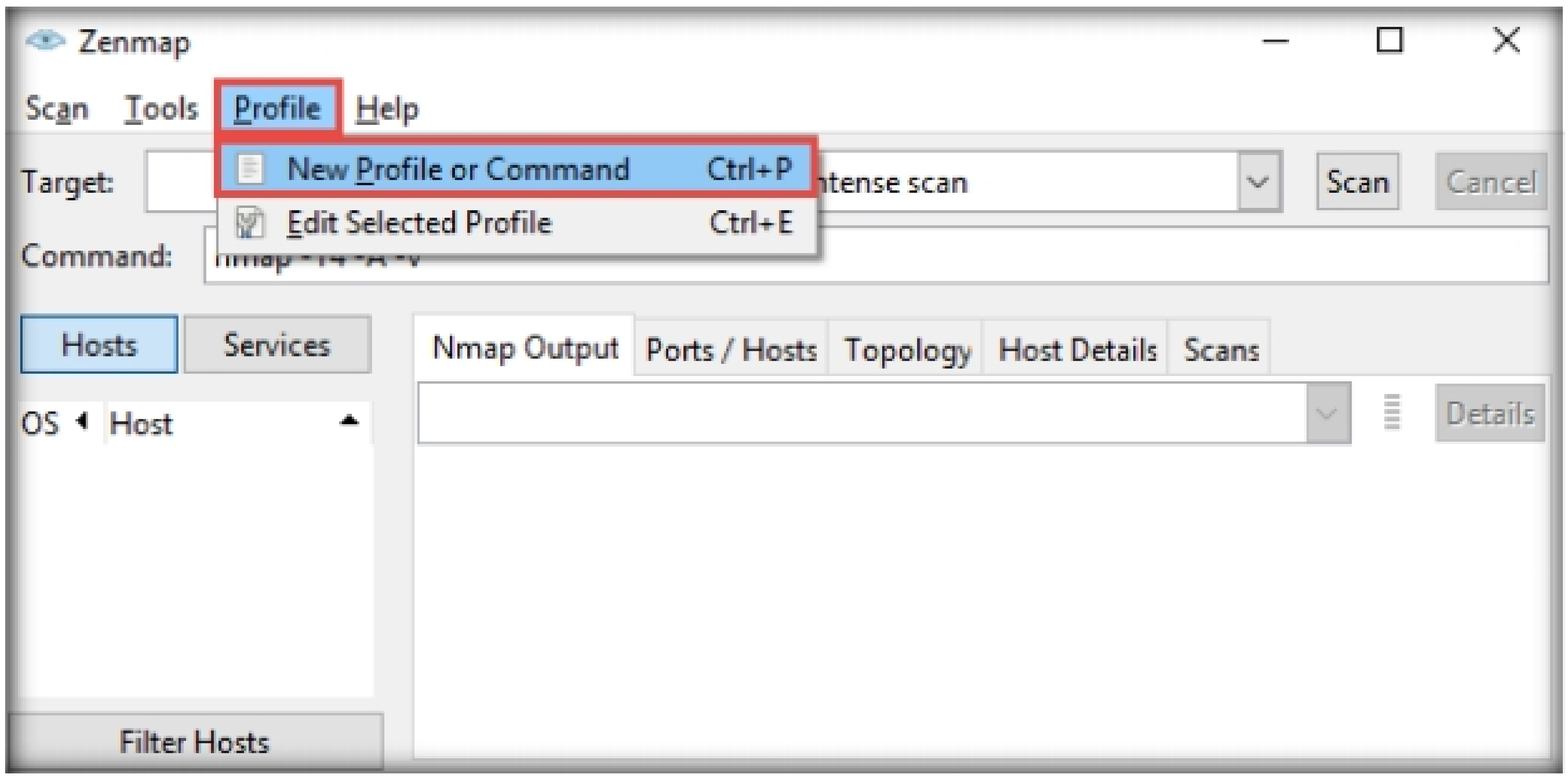
Figure 2.3.11: Zenmap Default Scan Options

TASK 3.7

Create a Scan Profile

29. To create a scan profile; click **Profile** → **New Profile or Command**.

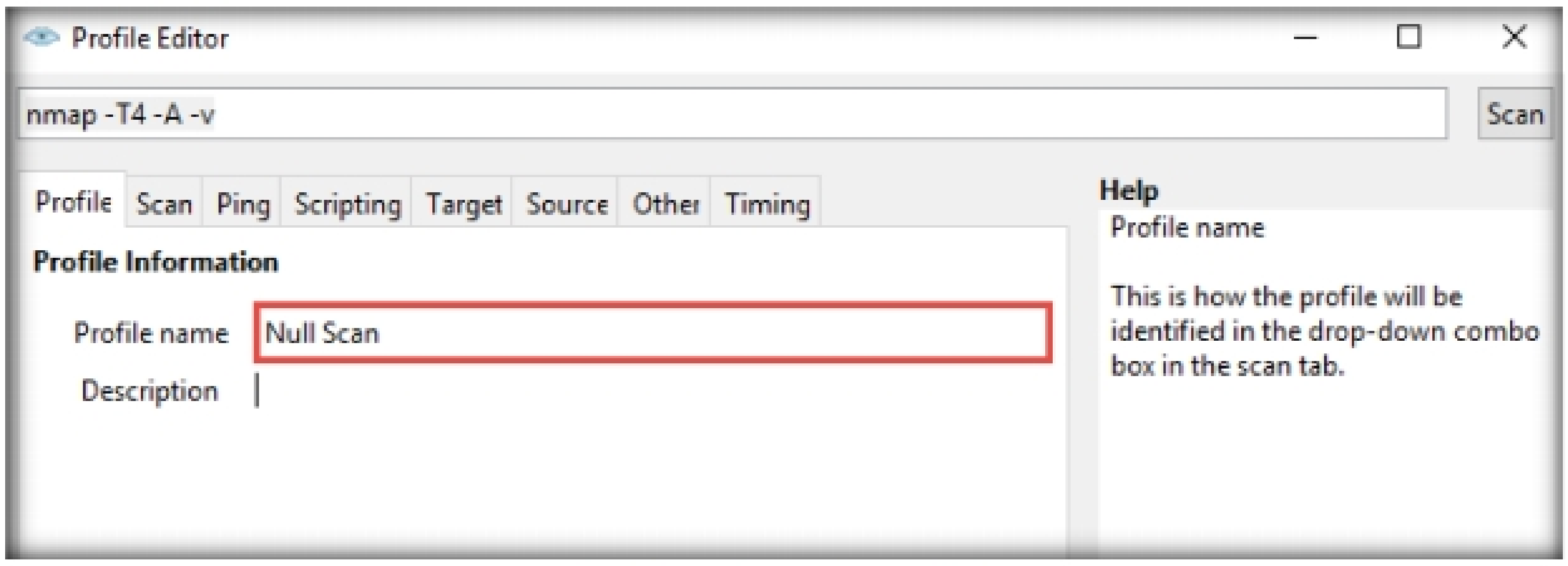
Note: If a **User Account Control** pop-up appears, click **Yes**.



Zenmap
Scan Tools Profile Help
New Profile or Command Ctrl+P
Edit Selected Profile Ctrl+E
Target:
Command:
ntense scan
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
Details
Filter Hosts

Figure 2.3.12: Creating a New Profile

30. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.



Profile Editor
Scan
Profile
Scan
Ping
Scripting
Target
Source
Other
Timing
Profile Information
Help

```
nmap -T4 -A -v
```

Profile name: Null Scan

Description:

Profile name

This is how the profile will be identified in the drop-down combo box in the scan tab.

Figure 2.3.13: Entering Profile Name

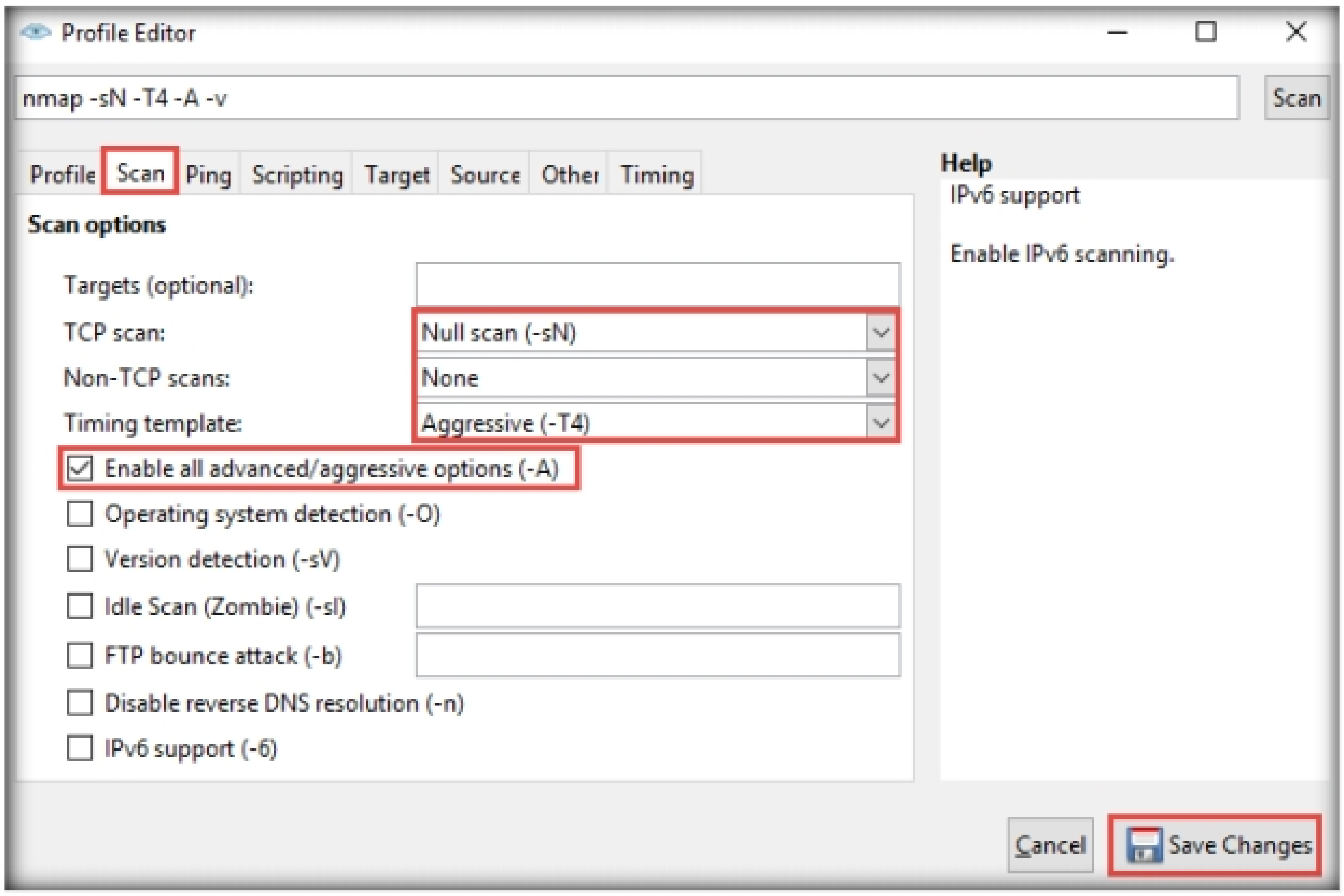
31. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.

32. Select **None** in the **Non-TCP scans** drop-down list and **Aggressive (-T4)** in the **Timing template** list. Ensure that the **Enable all advanced/aggressive options (-A)** checkbox is selected and click **Save Changes**, as shown in the screenshot.

Note: Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

33. This will create a new profile, and will thus be added to the profile list.

Note: You can select any other scan options as per your requirements.



Profile Editor
Scan
Profile
Scan
Ping
Scripting
Target
Source
Other
Timing
Scan options
Help
Cancel
Save Changes

```
nmap -sN -T4 -A -v
```

Targets (optional):

TCP scan: Null scan (-sN)

Non-TCP scans: None

Timing template: Aggressive (-T4)

☑ Enable all advanced/aggressive options (-A)

☐ Operating system detection (-O)

☐ Version detection (-sV)

☐ Idle Scan (Zombie) (-sI)

☐ FTP bounce attack (-b)

☐ Disable reverse DNS resolution (-n)

☐ IPv6 support (-6)

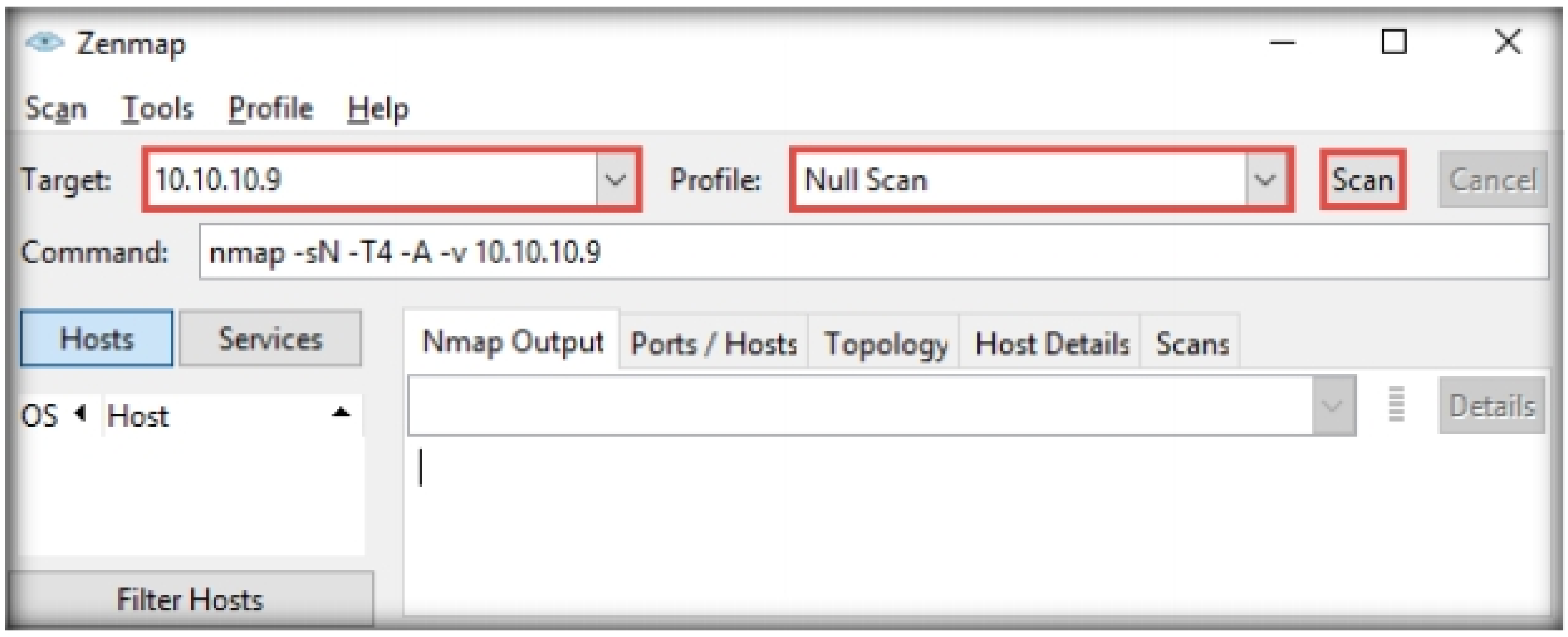
IPv6 support

Enable IPv6 scanning.

Figure 2.3.14: Configuring Null Scan Profile

34. In this task, we will be targeting the **Ubuntu** virtual machine (**10.10.10.9**). Therefore, before starting this task, turn on the **Ubuntu** virtual machine.

35. In the main window of **Zenmap**, enter the target IP address (here, **10.10.10.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.

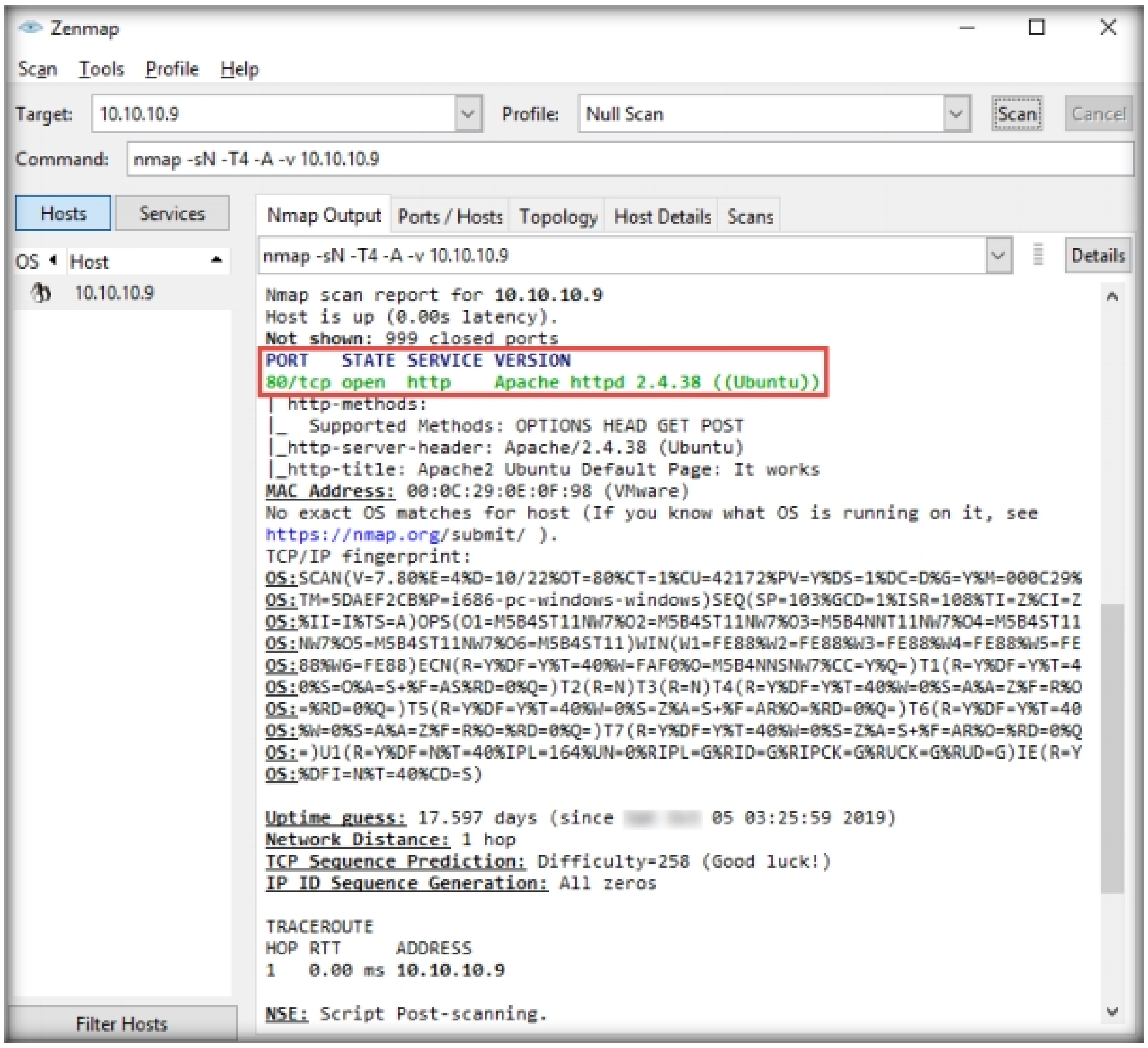

Zenmap
Scan
Tools
Profile
Help
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
Filter Hosts

Target: 10.10.10.9
Profile: Null Scan
Command: nmap -sN -T4 -A -v 10.10.10.9

Figure 2.3.15: Initiating Null Scan

36. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.

Note: The results obtained in your lab environment may differ.


Zenmap
Scan
Tools
Profile
Help
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
10.10.10.9
Filter Hosts

Target: 10.10.10.9
Profile: Null Scan
Command: nmap -sN -T4 -A -v 10.10.10.9

```
nmap -sN -T4 -A -v 10.10.10.9
Nmap scan report for 10.10.10.9
Host is up (0.00s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:0E:0F:98 (VMware)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/22%OT=80%CT=1%CU=42172%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=5DAEF2CB%P=i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z
OS:%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11
OS:NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE
OS:88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Uptime guess: 17.597 days (since [redacted] 05 03:25:59 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.00 ms 10.10.10.9

NSE: Script Post-scanning.
```

Figure 2.3.16: Null Scan Result

37. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.

    - **IDLE/IPID Header Scan**: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.

      # nmap -sI -v <target IP address>

    - **SCTP INIT Scan**: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

      # nmap -sY -v <target IP address>

    - **SCTP COOKIE ECHO Scan**: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

      # nmap -sZ -v <target IP address>

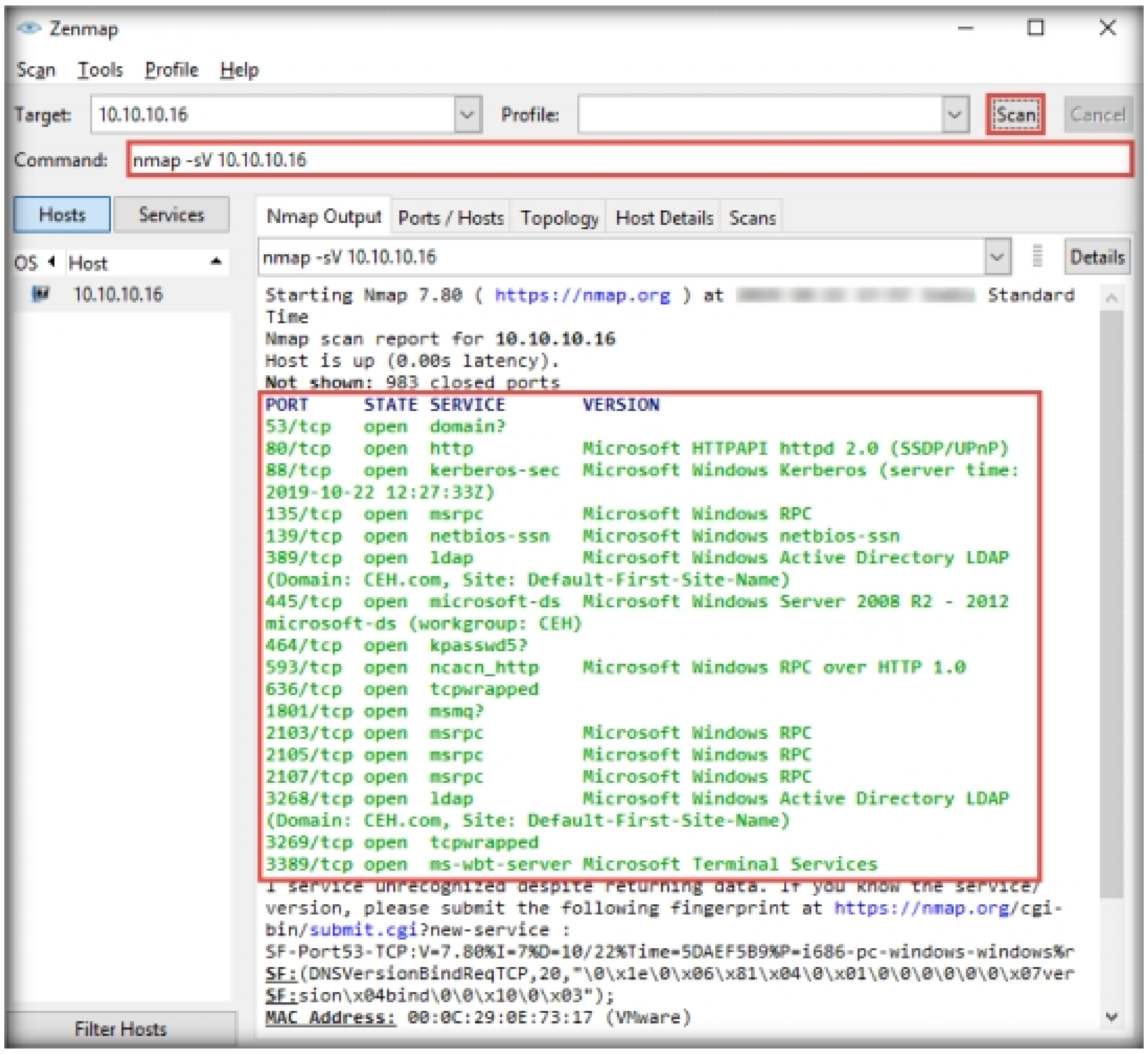
TASK 3.8

Perform Service Version Discovery

38. In the **Command** field, type the command **nmap -sV <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV**: detects service versions.

39. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.



Target: 10.10.10.16

Command: nmap -sV 10.10.10.16

```
nmap -sV 10.10.10.16
```

```
Starting Nmap 7.80 ( https://nmap.org ) at [redacted] Standard
Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2019-10-22 12:27:33Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: CEH.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: CEH)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP
(Domain: CEH.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/
version, please submit the following fingerprint at https://nmap.org/cgi-
bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=10/22%Time=5DAEF5B9%P=i686-pc-windows-windows%r
SF:(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07ver
SF:sion\x04bind\0\0\x10\0\x03");
MAC Address: 00:0C:29:0E:73:17 (VMware)
```

Figure 2.3.17: Zenmap scan results for Service Version Discovery

Note: Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.

40. Before starting the next sub-task, ensure that the **Parrot Security** and **Ubuntu** virtual machines are turned on.

TASK 3.9

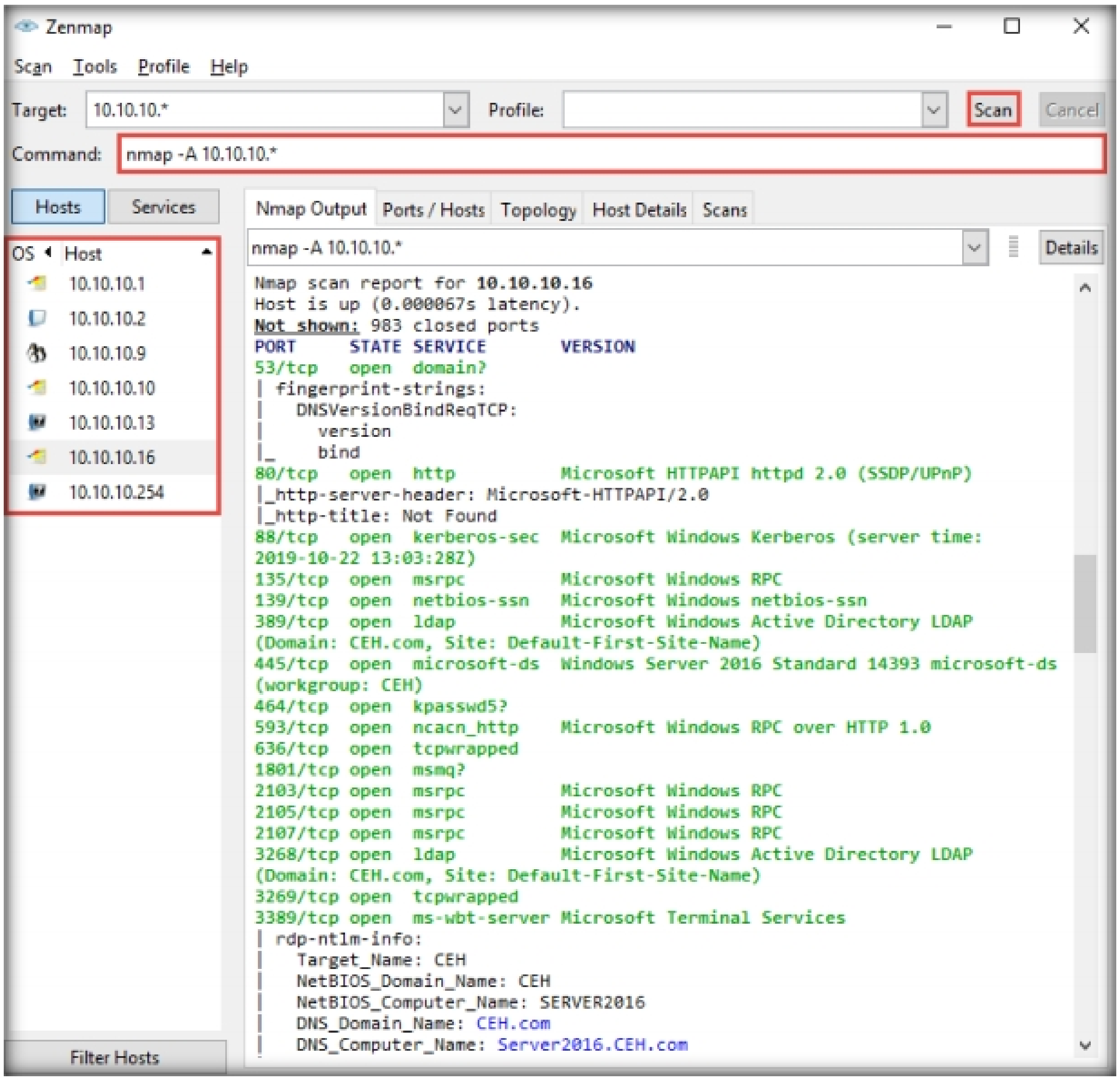
Scan a Whole Subnet

41. In the **Command** field, type the command **nmap -A <Target Subnet>** (here, target subnet is **10.10.10.***) and click **Scan**. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.

Note: **-A**: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

42. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot.

Note: This scan will take some time to finish the scanning process. The results might differ in your lab environment.



Target: 10.10.10.*

Command: nmap -A 10.10.10.*

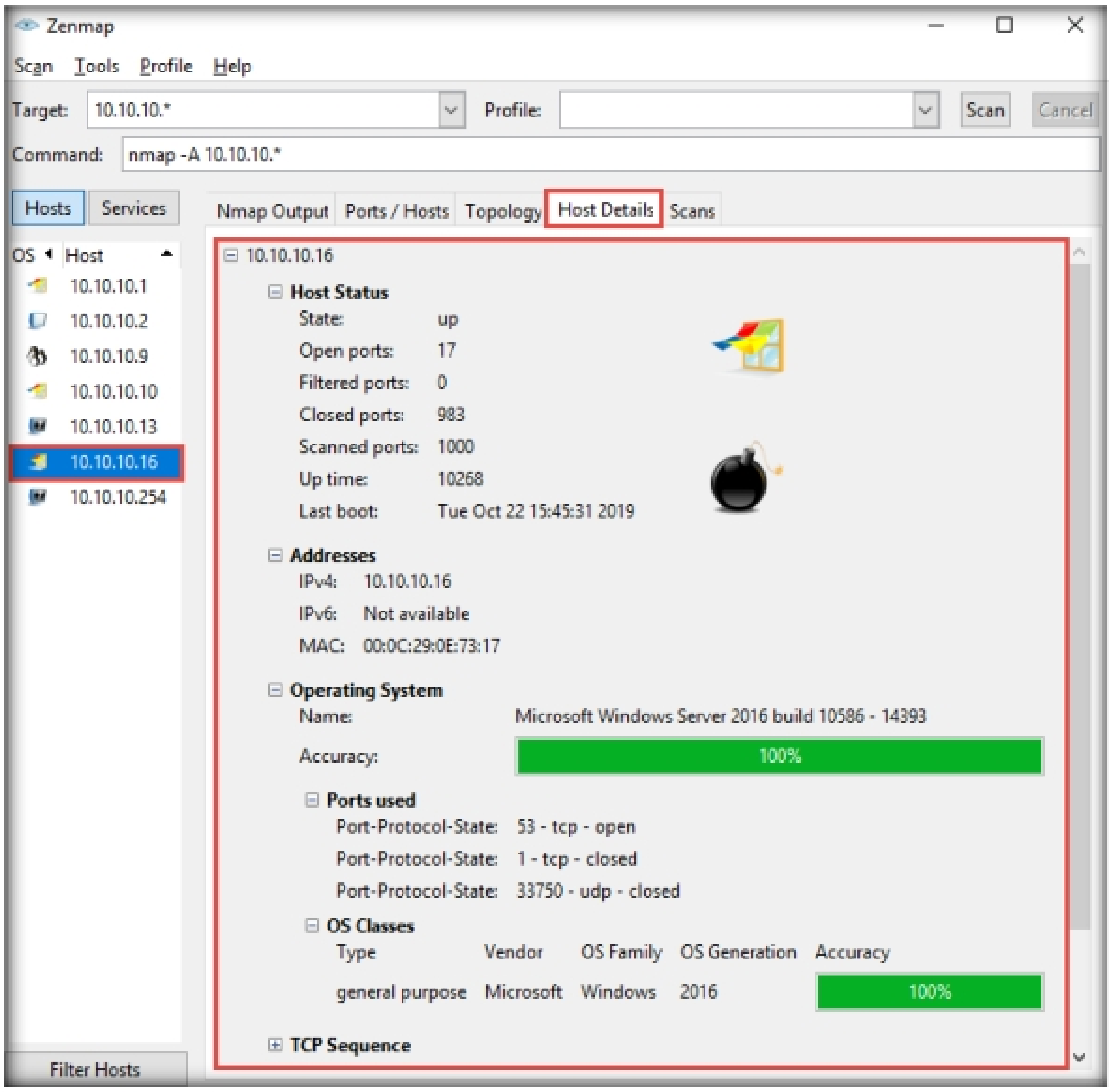
10.10.10.1
10.10.10.2
10.10.10.9
10.10.10.10
10.10.10.13
10.10.10.16
10.10.10.254

nmap -A 10.10.10.*

```
Nmap scan report for 10.10.10.16
Host is up (0.000067s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2019-10-22 13:03:28Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP
(Domain: CEH.com, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393 microsoft-ds
(workgroup: CEH)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1801/tcp open  msmq?
2103/tcp open  msrpc        Microsoft Windows RPC
2105/tcp open  msrpc        Microsoft Windows RPC
2107/tcp open  msrpc        Microsoft Windows RPC
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP
(Domain: CEH.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CEH
|   NetBIOS_Domain_Name: CEH
|   NetBIOS_Computer_Name: SERVER2016
|   DNS_Domain_Name: CEH.com
|   DNS_Computer_Name: Server2016.CEH.com
```

Figure 2.3.18: Zenmap displaying output for a Whole Subnet Scan

43. Choose an IP address **10.10.10.16** from the list of hosts in the left-pane and click the **Host Details** tab. This tab displays information such as **Host Status**, **Addresses**, **Operating System**, **Ports used**, **OS Classes**, etc. associated with the selected host.



Target: 10.10.10.*
Profile:
Command: nmap -A 10.10.10.*

10.10.10.1
10.10.10.2
10.10.10.9
10.10.10.10
10.10.10.13
10.10.10.16
10.10.10.254

10.10.10.16

Host Status
State: up
Open ports: 17
Filtered ports: 0
Closed ports: 983
Scanned ports: 1000
Up time: 10268
Last boot: Tue Oct 22 15:45:31 2019

Addresses
IPv4: 10.10.10.16
IPv6: Not available
MAC: 00:0C:29:0E:73:17

Operating System
Name: Microsoft Windows Server 2016 build 10586 - 14393
Accuracy: 100%

Ports used
Port-Protocol-State: 53 - tcp - open
Port-Protocol-State: 1 - tcp - closed
Port-Protocol-State: 33750 - udp - closed

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Microsoft	Windows	2016	100%

TCP Sequence

Figure 2.3.19: Zenmap displaying the Open Ports under Ports/Hosts tab

44. This concludes the demonstration of discovering target open ports, services, services versions, device type, OS details, etc. of the active hosts in the target network using various scanning techniques of Nmap.

45. Close all open windows and document all the acquired information.

46. Turn off the **Windows 10** and **Ubuntu** virtual machine.

TASK 4

Explore Various Network Scanning Techniques using Hping3

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

1. Switch to the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. Using Hping, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

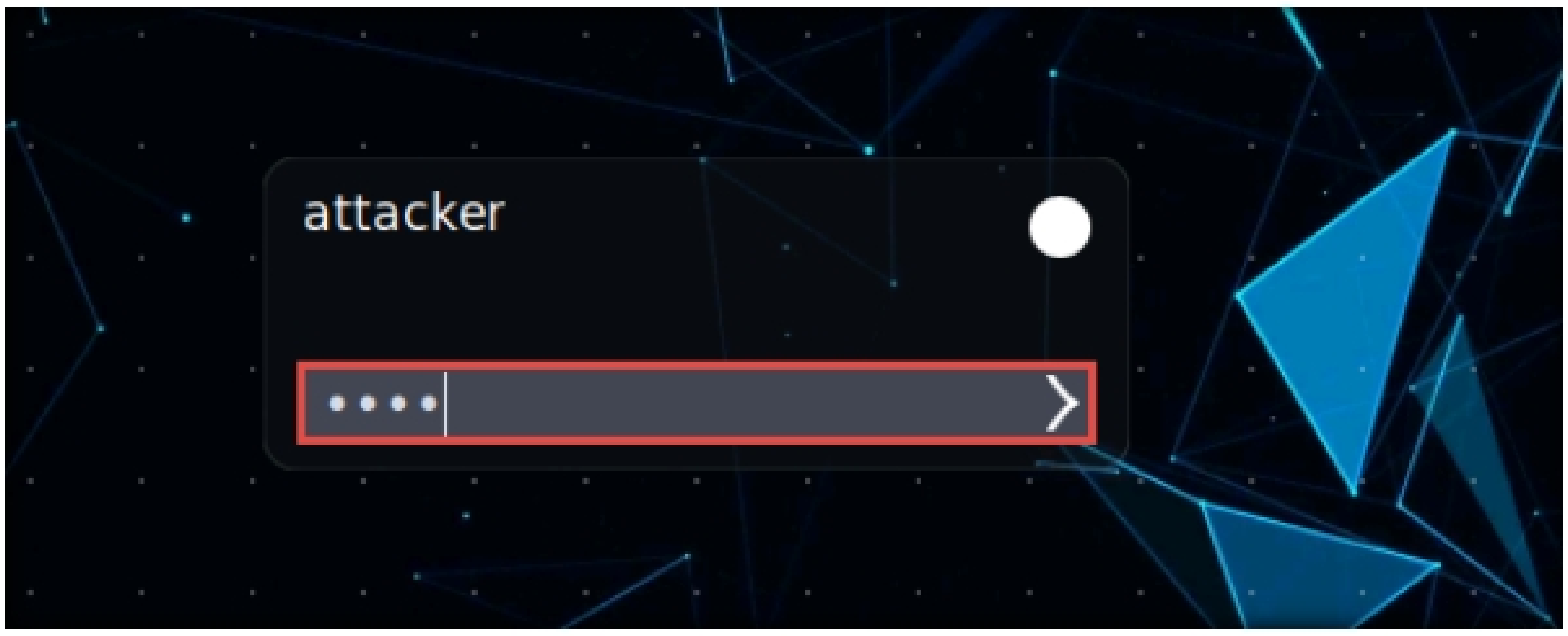


Figure 2.4.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

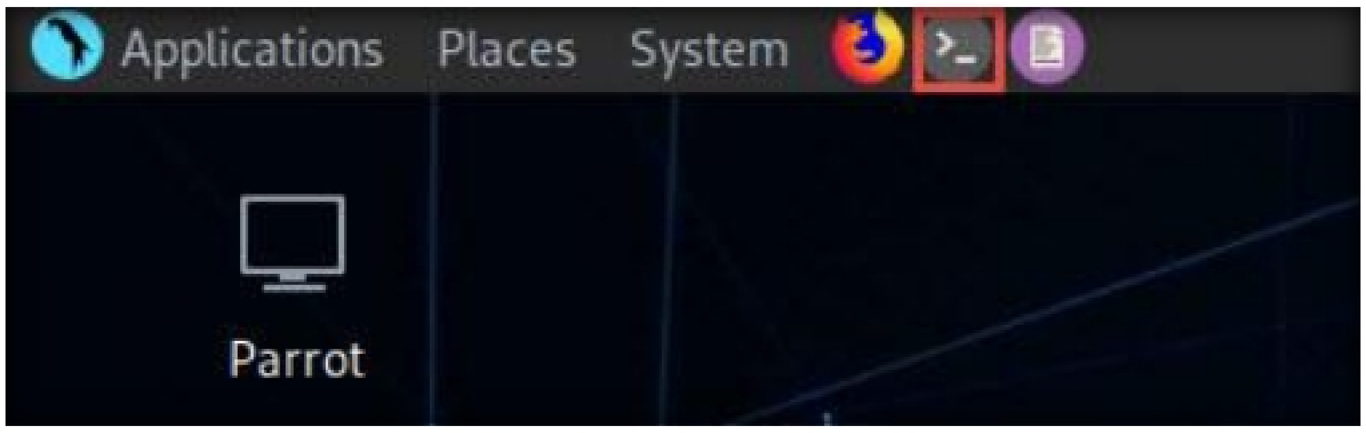
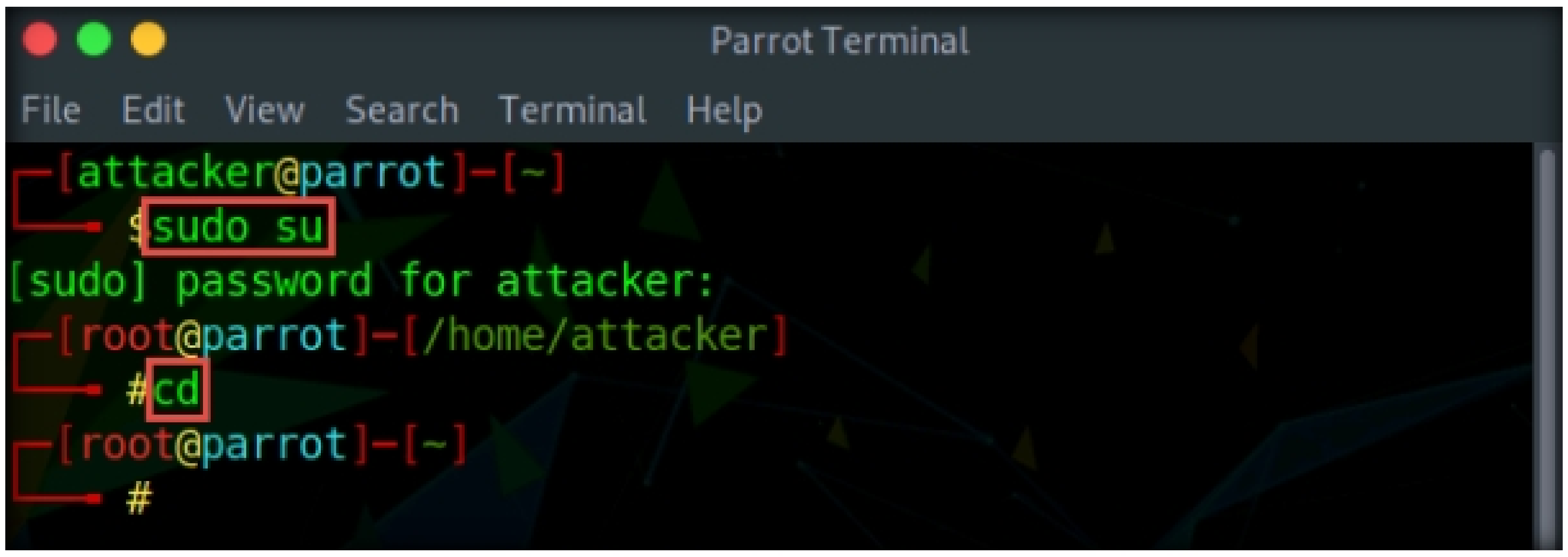


Figure 2.4.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

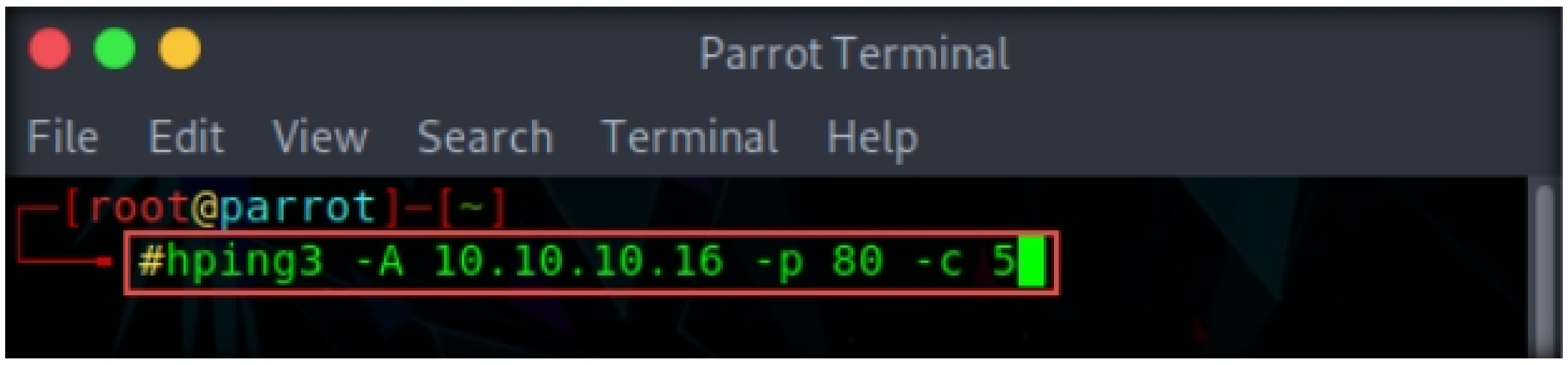
Figure 2.4.3: Running the programs as a root user

TASK 4.1

Perform ACK Scan

7. In the terminal window, type **hping3 -A <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

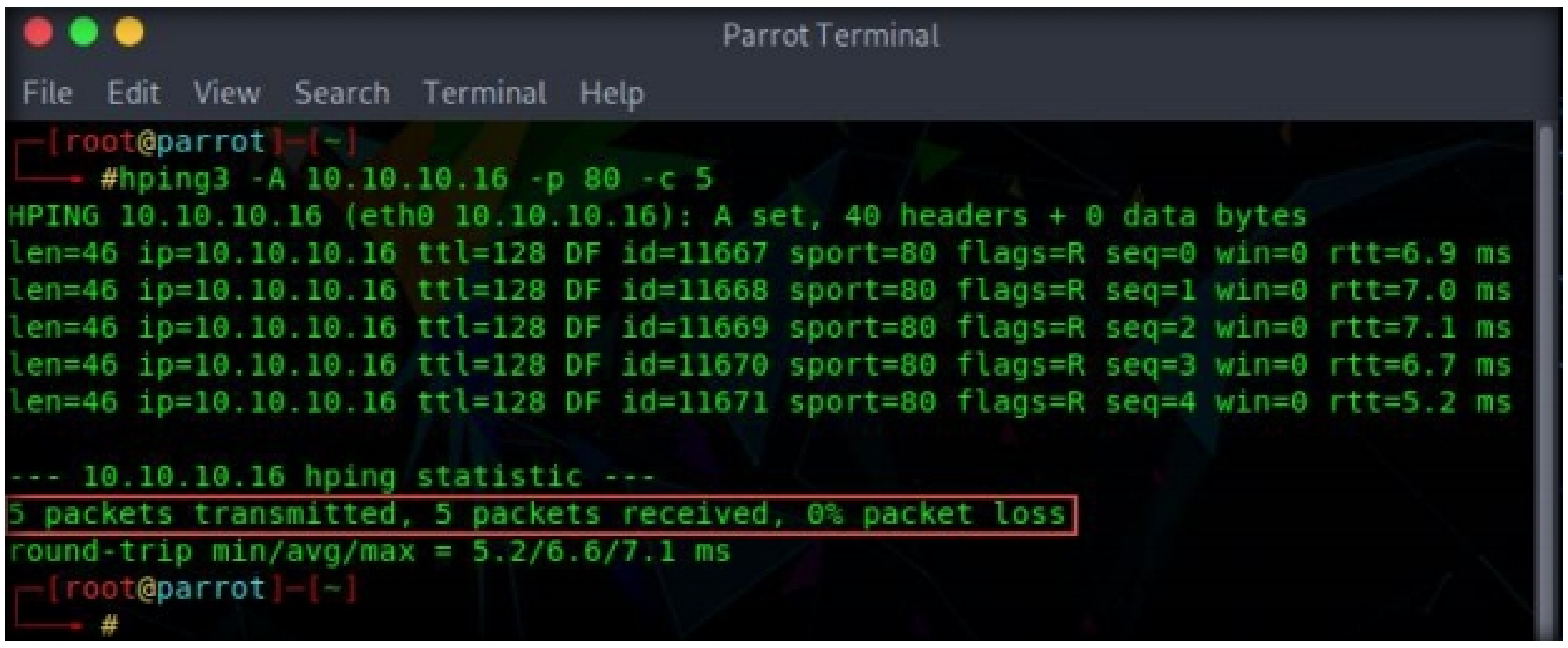
Note: In this command, **-A** specifies setting the ACK flag, **-p** specifies the port to be scanned (here, **80**), and **-c** specifies the packet count (here, **5**).



```
┌─[root@parrot]─[~]
└──╼ #hping3 -A 10.10.10.16 -p 80 -c 5
```

Figure 2.4.4: Hping3 TCP ACK scan command

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #hping3 -A 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): A set, 40 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 DF id=11667 sport=80 flags=R seq=0 win=0 rtt=6.9 ms
len=46 ip=10.10.10.16 ttl=128 DF id=11668 sport=80 flags=R seq=1 win=0 rtt=7.0 ms
len=46 ip=10.10.10.16 ttl=128 DF id=11669 sport=80 flags=R seq=2 win=0 rtt=7.1 ms
len=46 ip=10.10.10.16 ttl=128 DF id=11670 sport=80 flags=R seq=3 win=0 rtt=6.7 ms
len=46 ip=10.10.10.16 ttl=128 DF id=11671 sport=80 flags=R seq=4 win=0 rtt=5.2 ms

--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.2/6.6/7.1 ms
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.4.5: Hping3 ACK scan result

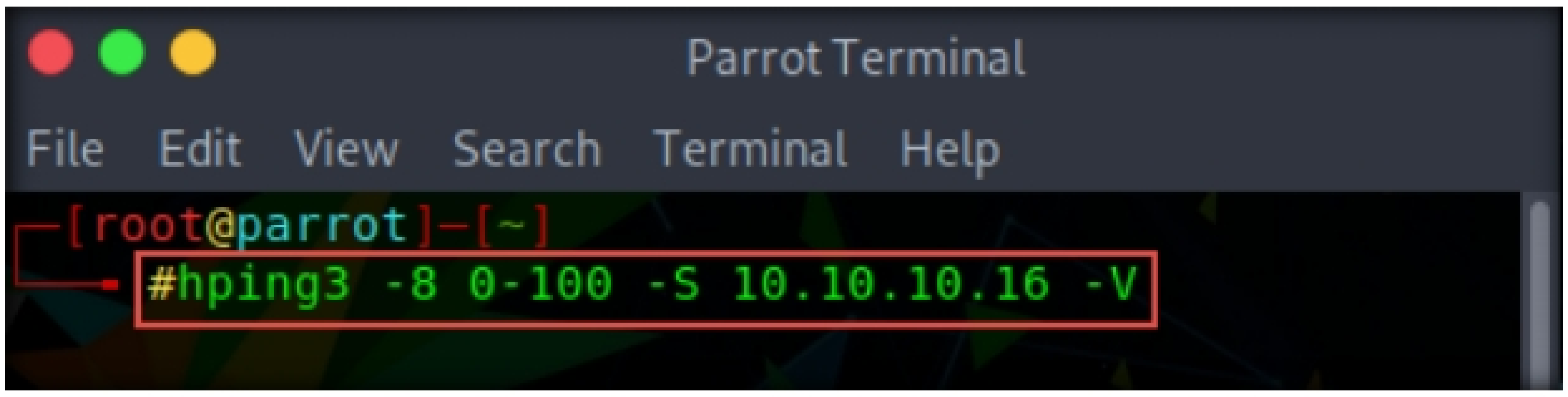
Note: The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

TASK 4.2

Perform SYN Scan

9. In the terminal window, type **hping3 -8 0-100 -S <Target IP Address> -V** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

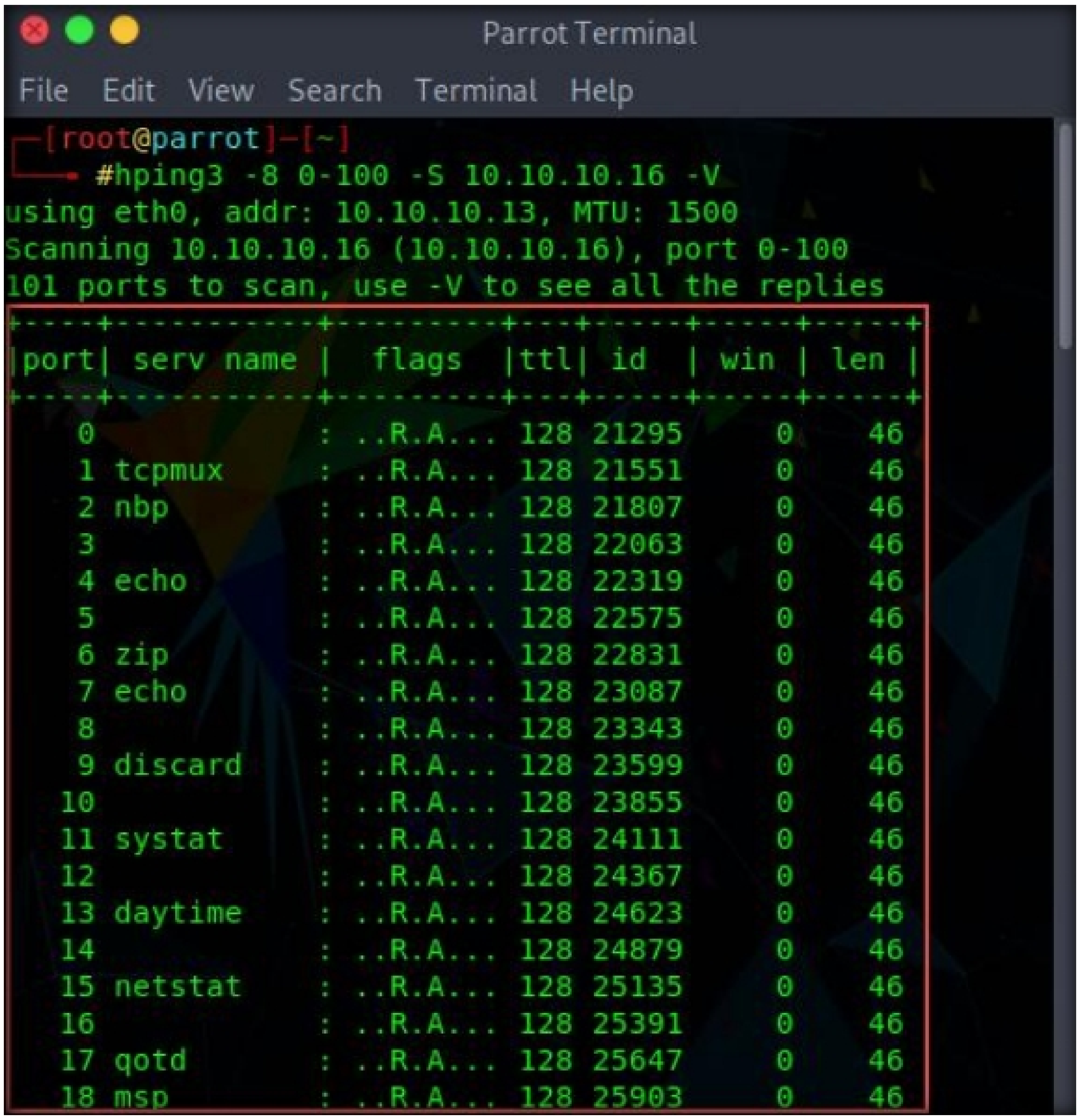
Note: In this command, **-8** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.



```
┌─[root@parrot]─[~]
└──╼ #hping3 -8 0-100 -S 10.10.10.16 -V
```

Figure 2.4.6: Hping3 TCP SYN scan command

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #hping3 -8 0-100 -S 10.10.10.16 -V
using eth0, addr: 10.10.10.13, MTU: 1500
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
    0           : ..R.A... 128 21295     0    46
    1 tcpmux    : ..R.A... 128 21551     0    46
    2 nbp       : ..R.A... 128 21807     0    46
    3           : ..R.A... 128 22063     0    46
    4 echo      : ..R.A... 128 22319     0    46
    5           : ..R.A... 128 22575     0    46
    6 zip       : ..R.A... 128 22831     0    46
    7 echo      : ..R.A... 128 23087     0    46
    8           : ..R.A... 128 23343     0    46
    9 discard   : ..R.A... 128 23599     0    46
   10           : ..R.A... 128 23855     0    46
   11 systat    : ..R.A... 128 24111     0    46
   12           : ..R.A... 128 24367     0    46
   13 daytime   : ..R.A... 128 24623     0    46
   14           : ..R.A... 128 24879     0    46
   15 netstat   : ..R.A... 128 25135     0    46
   16           : ..R.A... 128 25391     0    46
   17 qotd      : ..R.A... 128 25647     0    46
   18 msp       : ..R.A... 128 25903     0    46
```

Figure 2.4.7: Hping3 SYN scan result

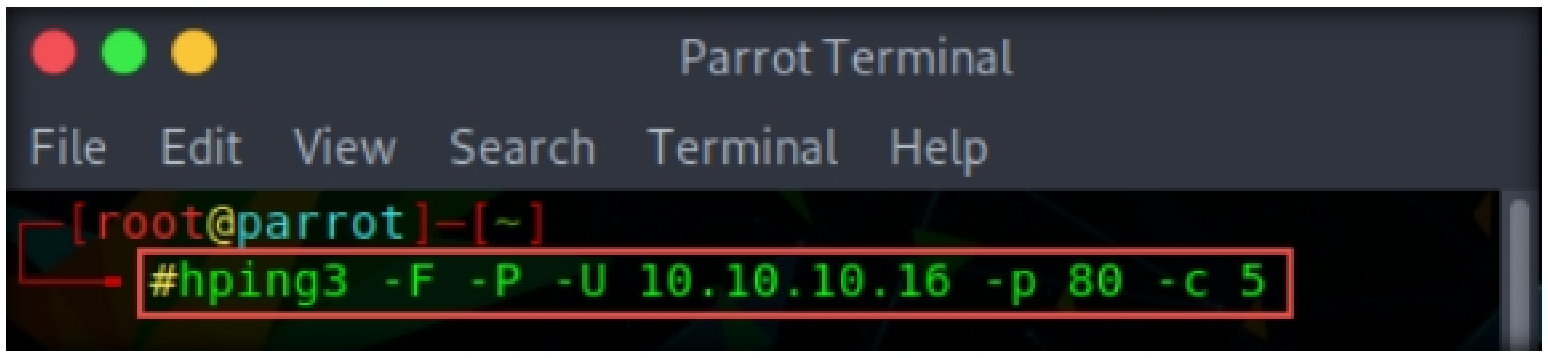
Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

TASK 4.3

Perform FIN, PUSH, and URG Scan

11. In the terminal window, type **hping3 -F -P -U <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

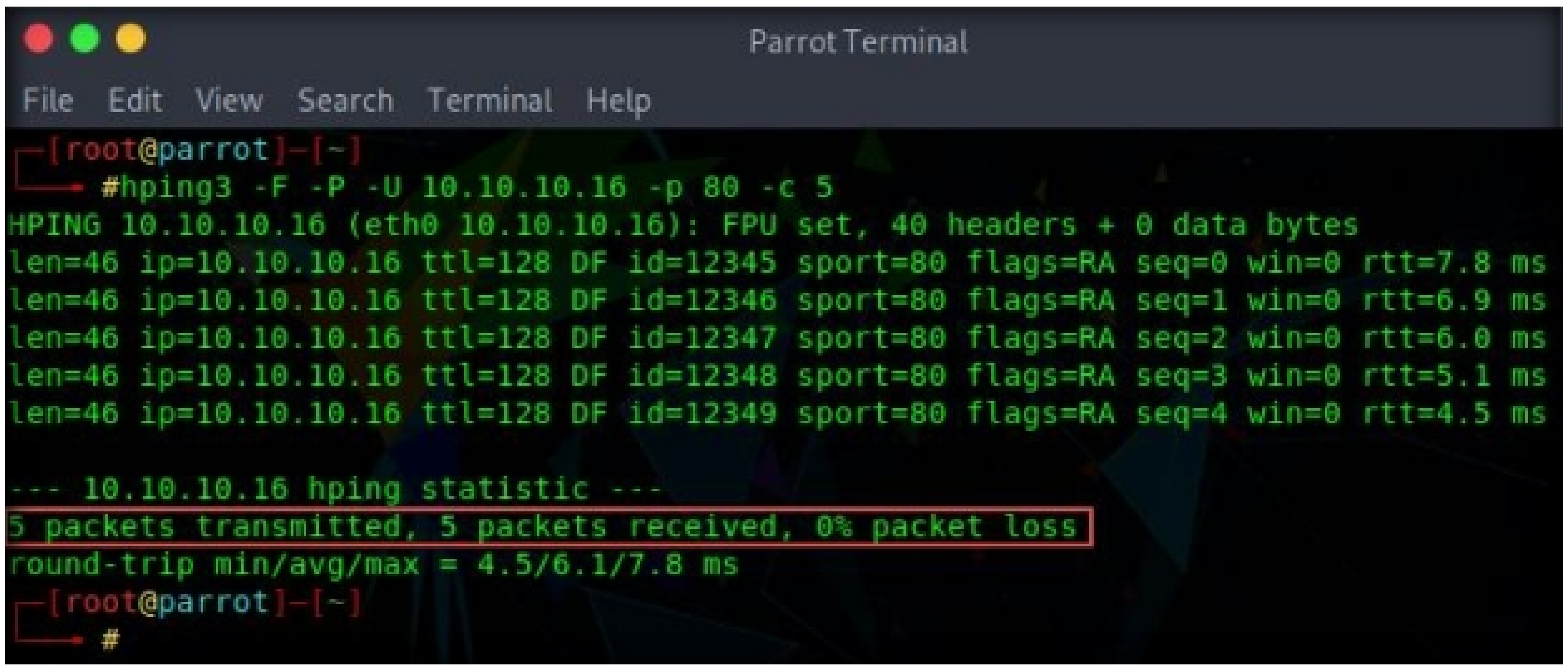
Note: In this command, **-F** specifies setting the FIN flag, **-P** specifies setting the PUSH flag, **-U** specifies setting the URG flag, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).



```
┌─[root@parrot]─[~]
└──╼ #hping3 -F -P -U 10.10.10.16 -p 80 -c 5
```

Figure 2.4.8: Hping3 FIN, PUSH, and URG scan command

12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 DF id=12345 sport=80 flags=RA seq=0 win=0 rtt=7.8 ms
len=46 ip=10.10.10.16 ttl=128 DF id=12346 sport=80 flags=RA seq=1 win=0 rtt=6.9 ms
len=46 ip=10.10.10.16 ttl=128 DF id=12347 sport=80 flags=RA seq=2 win=0 rtt=6.0 ms
len=46 ip=10.10.10.16 ttl=128 DF id=12348 sport=80 flags=RA seq=3 win=0 rtt=5.1 ms
len=46 ip=10.10.10.16 ttl=128 DF id=12349 sport=80 flags=RA seq=4 win=0 rtt=4.5 ms

--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.5/6.1/7.8 ms
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.4.9: Hping3 FIN, PUSH, and URG scan result

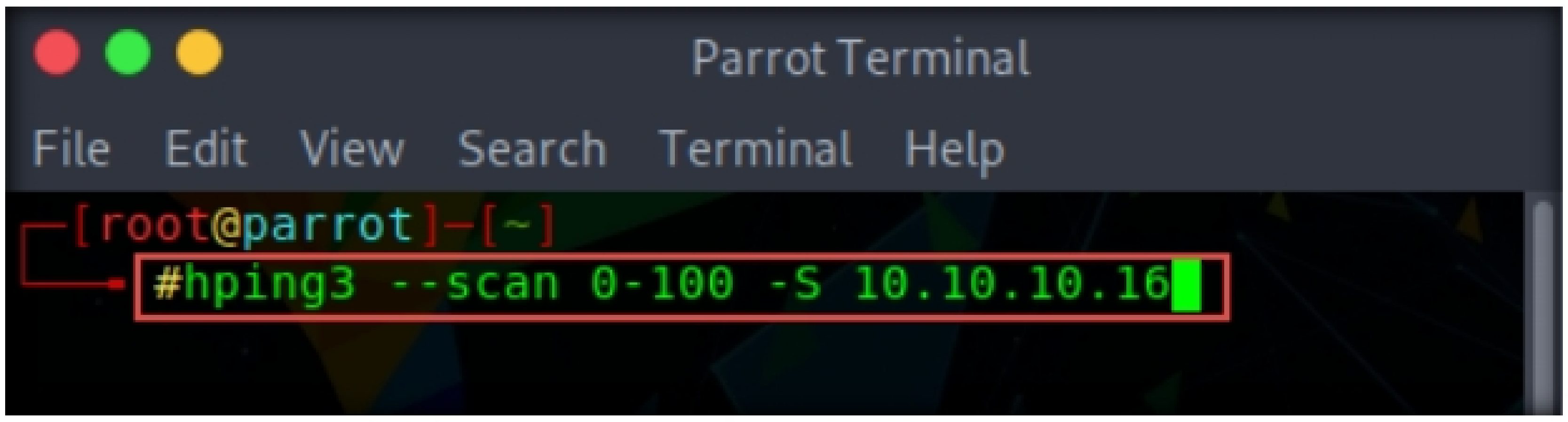
Note: FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will not receive a response. If the port is closed, Hping will return an RST response.

TASK 4.4

Perform TCP Stealth Scan

13. In the terminal window, type **hping3 --scan 0-100 -S <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

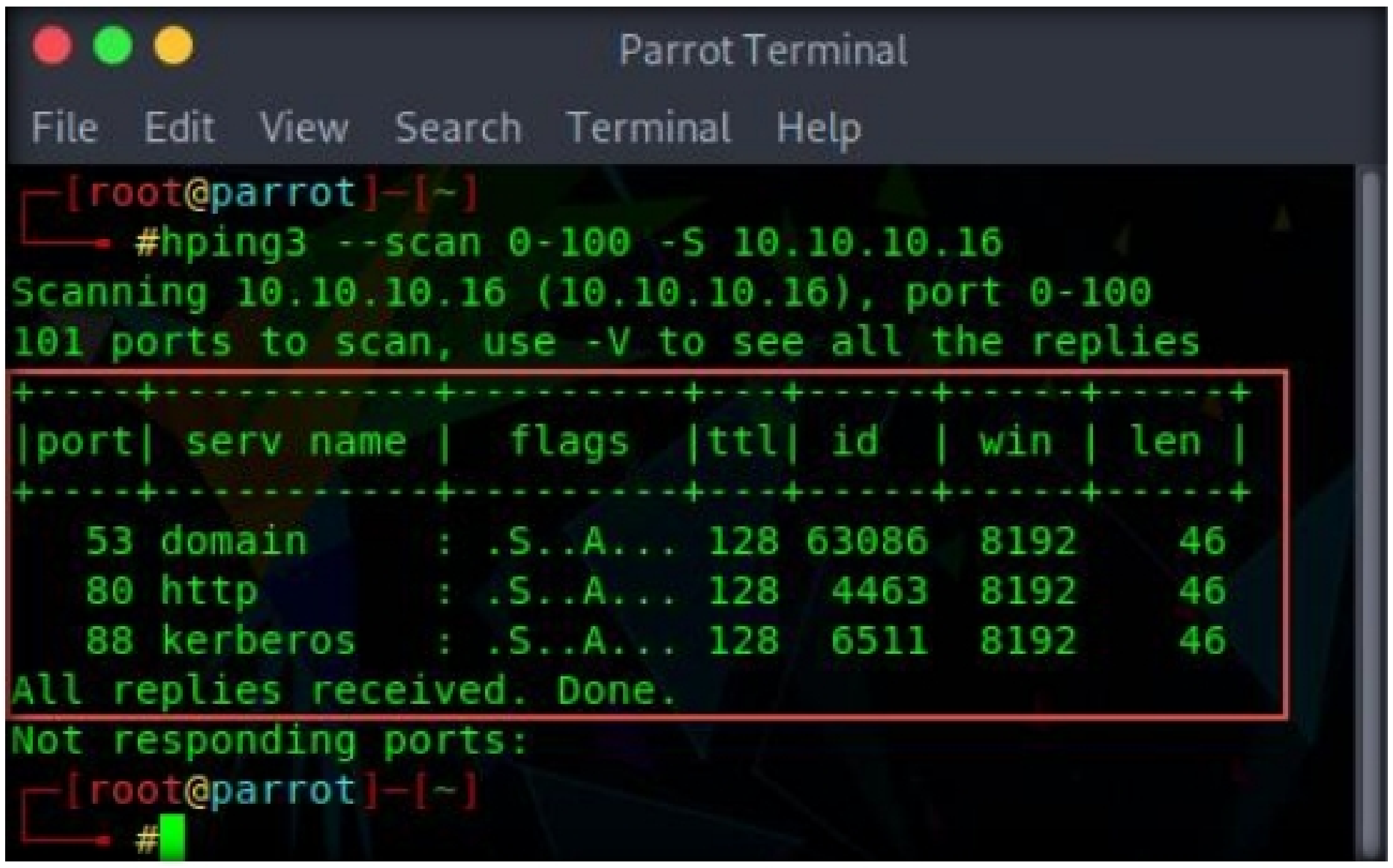
Note: In this command, **--scan** specifies the port range to scan, **0-100** specifies the range of ports to be scanned, and **-S** specifies setting the SYN flag.



```
┌─[root@parrot]─[~]
└──╼ #hping3 --scan 0-100 -S 10.10.10.16
```

Figure 2.4.10: Hping3 TCP stealth scan command

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #hping3 --scan 0-100 -S 10.10.10.16
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A... 128 63086  8192    46
   80 http       : .S..A... 128  4463  8192    46
   88 kerberos   : .S..A... 128  6511  8192    46
All replies received. Done.
Not responding ports:
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.4.11: Hping3 TCP stealth scan result

Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

15. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.
    - ICMP scan: **hping3 -1 <Target IP Address> -p 80 -c 5**
    - Entire subnet scan for live host: **hping3 -1 <Target Subnet> –rand-dest -I eth0**
    - UDP scan: **hping3 -2 <Target IP Address> -p 80 -c 5**
16. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** and **Windows Server 2016** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Perform OS Discovery

Banner grabbing, or OS fingerprinting, is used to determine the OS running on a remote target system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system's vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Identify the target system's OS with Time-to-Live (TTL) and TCP window sizes using Wireshark
- Perform OS discovery using Nmap Script Engine (NSE)
- Perform OS discovery using Unicornscan

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Wireshark located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark**
- You can also download the latest version of Wireshark from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 15 Minutes

Overview of OS Discovery/Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing**

  Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

- **Passive Banner Grabbing**

  This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System (OS)	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

Lab Tasks

TASK 1

Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Here, we will use the Wireshark tool to perform OS discovery on the target host(s).

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, and **Ubuntu** virtual machine.
2. In the **Windows 10** virtual machine log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

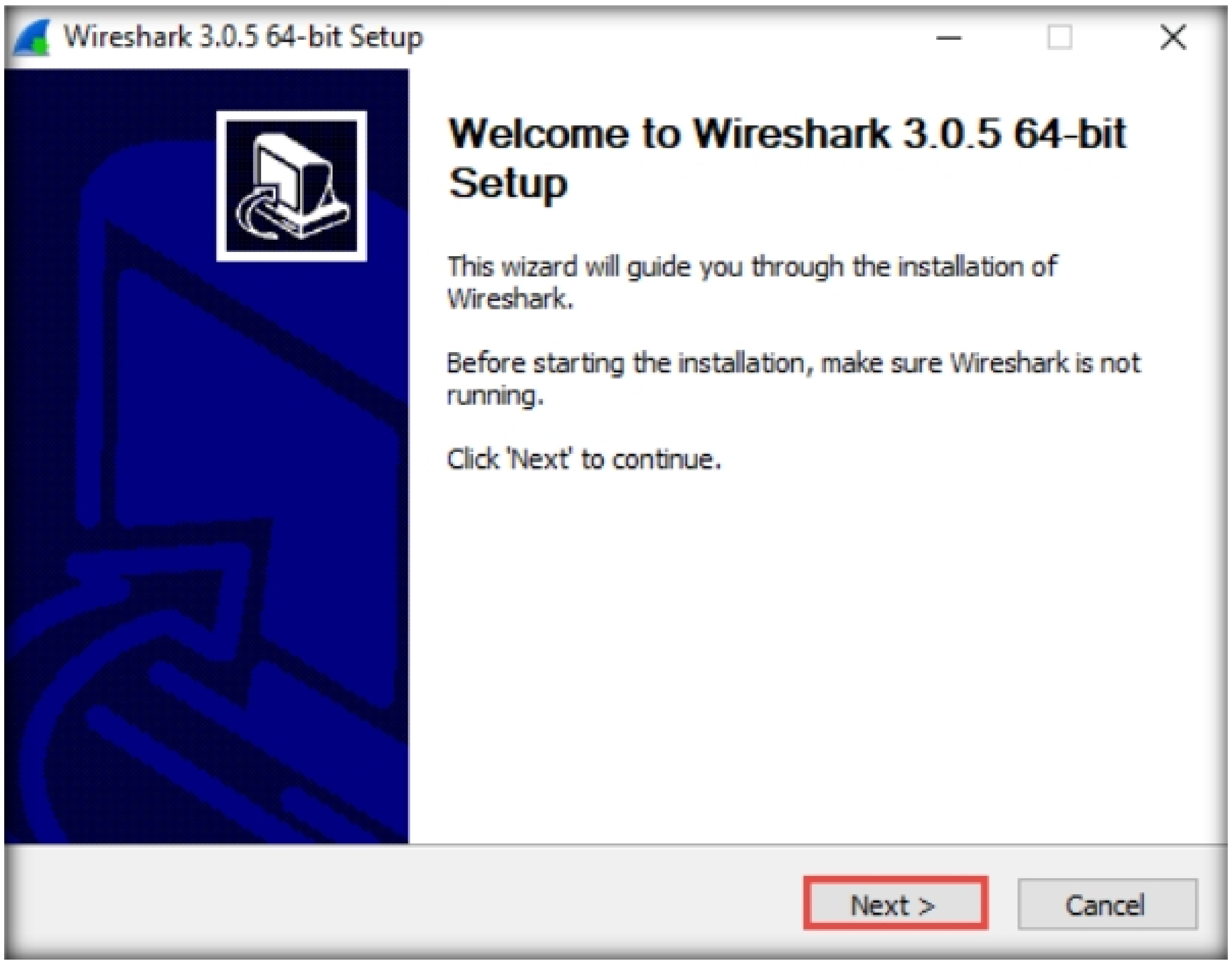
Install Wireshark

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-win64-3.0.5.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Wireshark is a network protocol analyzer that allows capturing and interactively browsing the traffic running on a computer network. It is used to identify the target OS through sniffing/capturing the response generated from the target machine to the request-originated machine. Further, you can observe the TTL and TCP window size fields in the captured TCP packet. Using these values, the target OS can be determined.

4. **Wireshark Setup** window appears; follow the steps to install Wireshark using all default settings.



Welcome to Wireshark 3.0.5 64-bit Setup

This wizard will guide you through the installation of Wireshark.

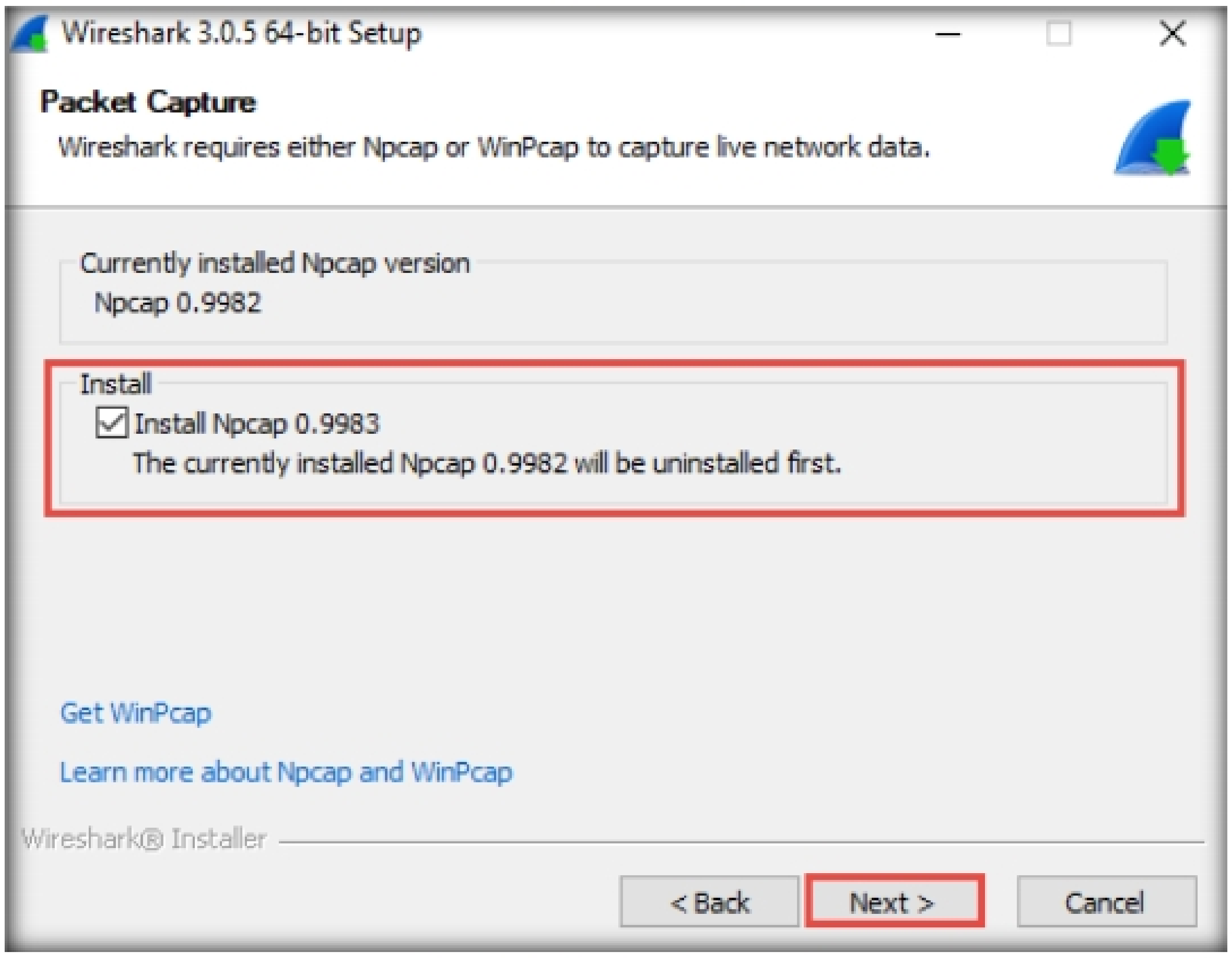
Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Figure 3.1.1: Wireshark Setup window

5. In the **Packet Capture** wizard, ensure that the **Install Npcap 0.9983** checkbox is selected and click **Next**.

Note: The version of Npcap may differ in your lab environment.



Wireshark 3.0.5 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap version

Npcap 0.9982

Install

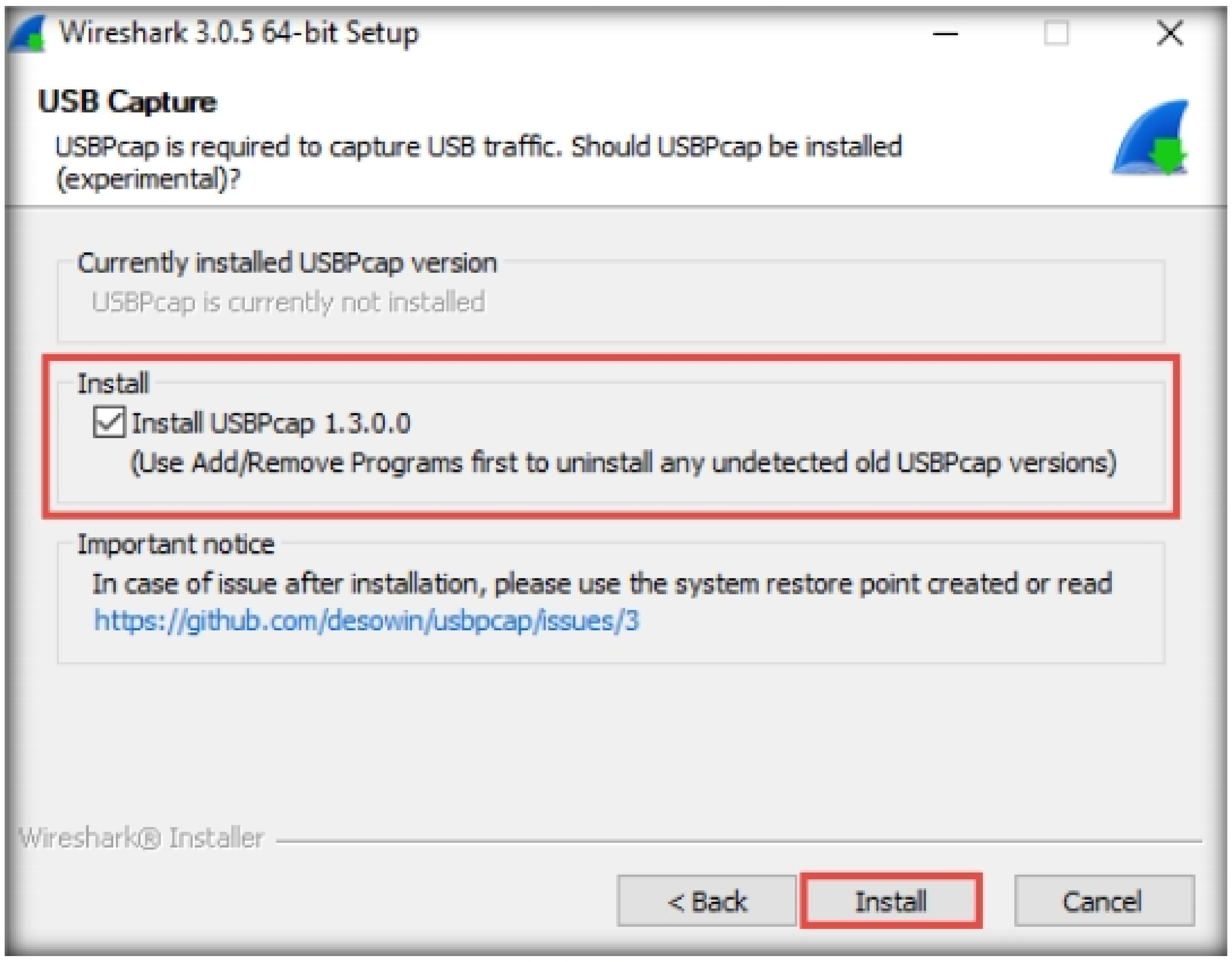
☑ Install Npcap 0.9983

The currently installed Npcap 0.9982 will be uninstalled first.

Figure 3.1.2: Packet Capture wizard

6. In the **USB Capture** wizard, select the **Install USBPcap 1.3.0.0** checkbox and click **Install**.

Note: The version of USBPcap may differ in your lab environment.



Wireshark 3.0.5 64-bit Setup

USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version

USBPcap is currently not installed

Install

☑ Install USBPcap 1.3.0.0

(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

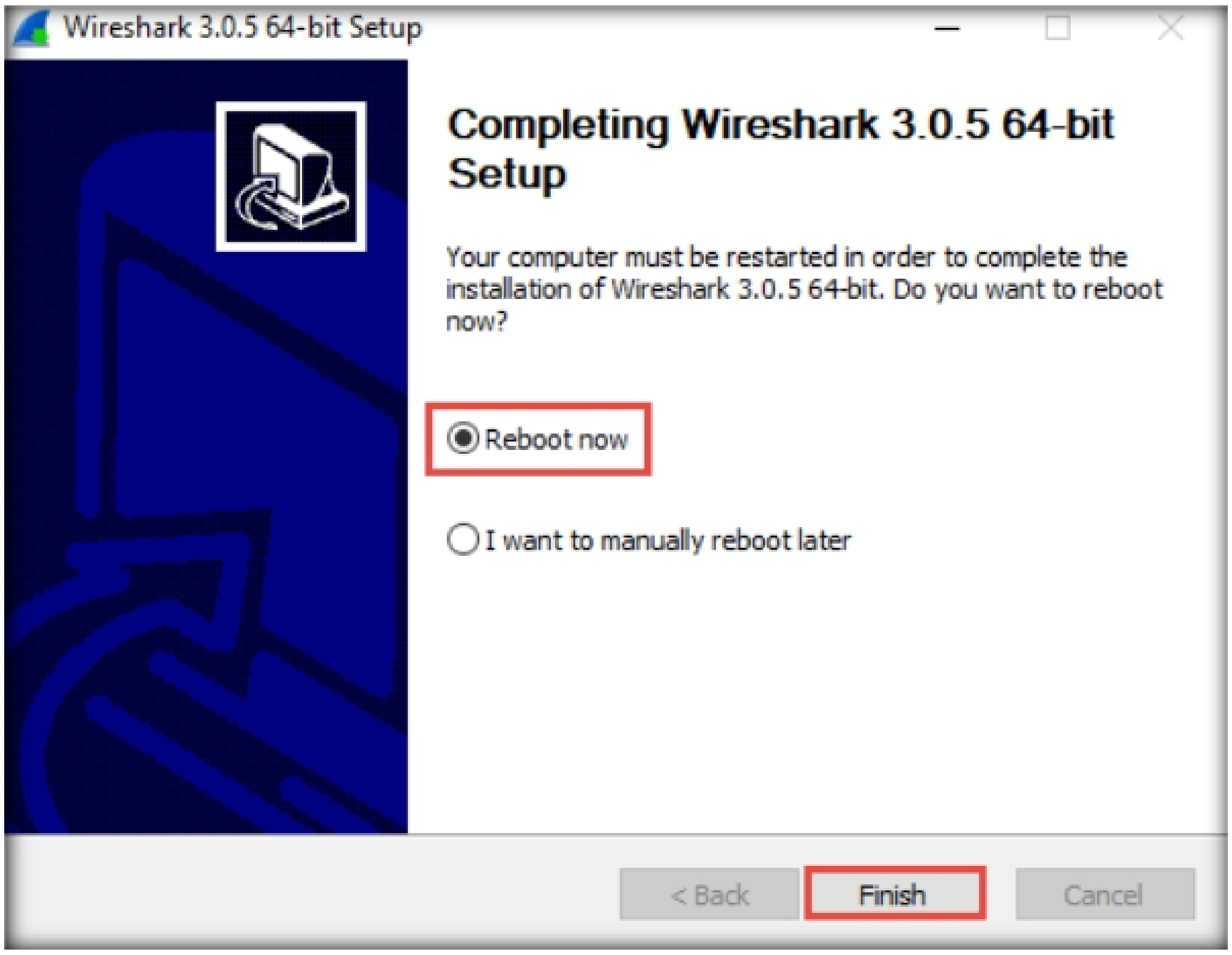
Important notice

In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

Figure 3.1.3: USB Capture wizard

7. Follow the wizard steps to install Npcap and USBPcap using all default settings.

8. After the completion of the installation, in the **Wireshark Setup** windows, ensure that the **Reboot now** radio button is selected, and click **Finish**.



Wireshark 3.0.5 64-bit Setup

Completing Wireshark 3.0.5 64-bit Setup

Your computer must be restarted in order to complete the installation of Wireshark 3.0.5 64-bit. Do you want to reboot now?

● Reboot now

○ I want to manually reboot later

Figure 3.1.4: Wireshark setup window

9. The **Windows 10** virtual machine will restart. Log in with the credentials **Admin/Pa$$w0rd**.

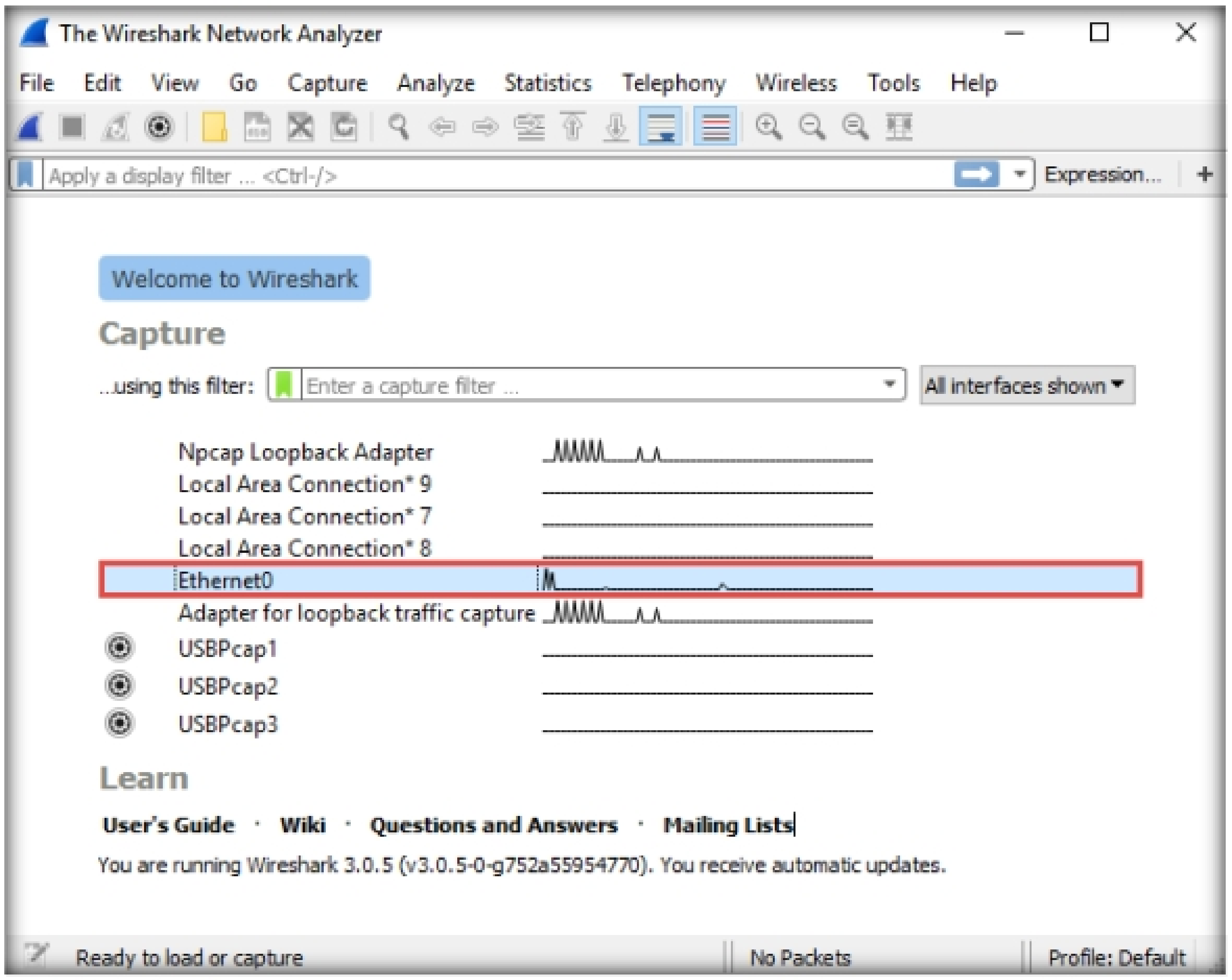
10. Click on the **Start** menu and launch **Wireshark** from the applications.

TASK 1.2

Run Wireshark

11. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

Note: The available interface might vary in your lab environment.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Npcap Loopback Adapter
Local Area Connection* 9
Local Area Connection* 7
Local Area Connection* 8
Ethernet0
Adapter for loopback traffic capture
USBPcap1
USBPcap2
USBPcap3
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

You are running Wireshark 3.0.5 (v3.0.5-0-g752a55954770). You receive automatic updates.

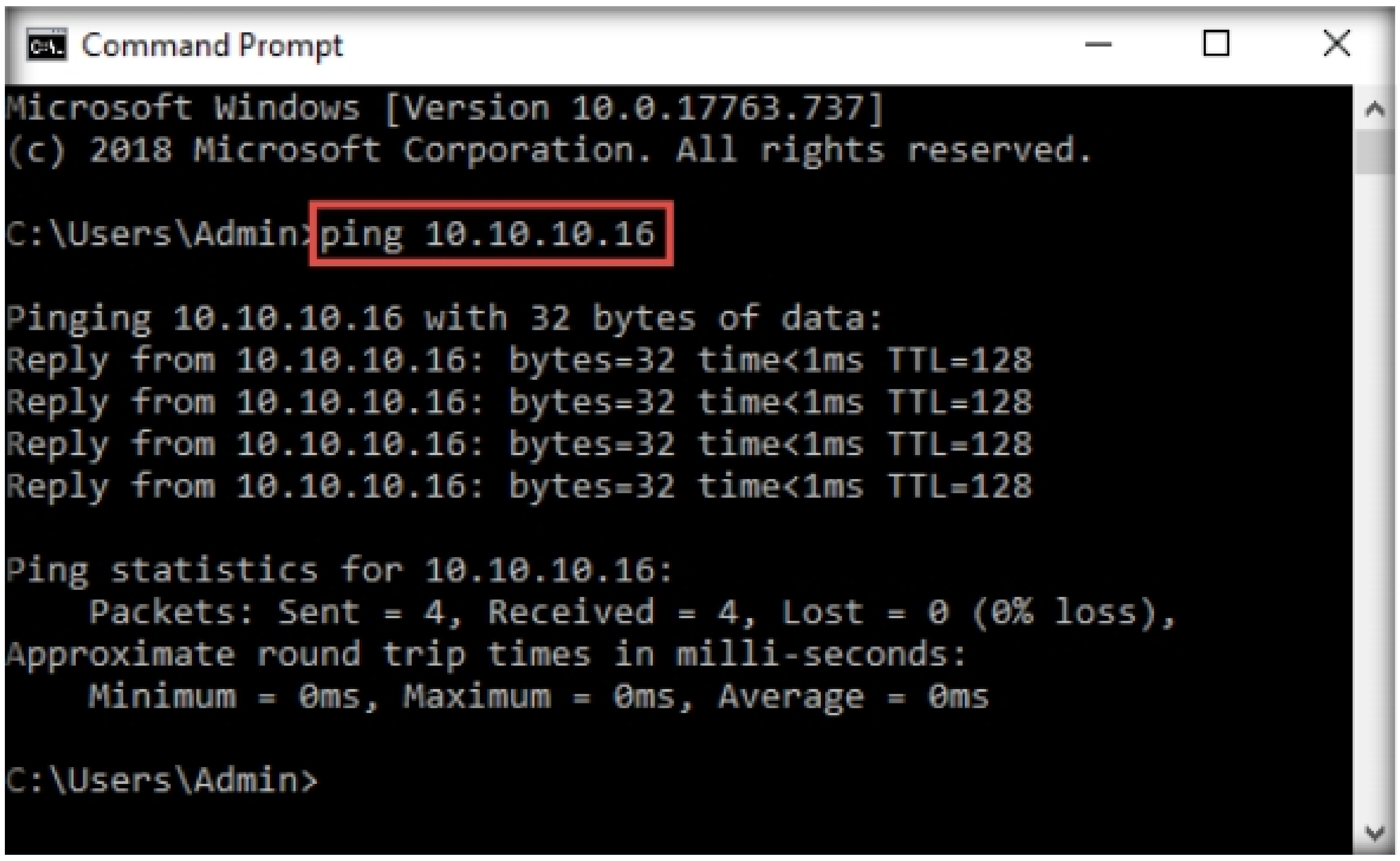
Figure 3.1.5: Wireshark main window, enabling to start the capture

TASK 1.3

Perform Ping on Target Machine (Windows)

12. Open the **Command Prompt**, type **ping 10.10.10.16** and press **Enter**.

Note: **10.10.10.16** is the IP address of the **Windows Server 2016** virtual machine; this may vary in your lab environment.


Command Prompt

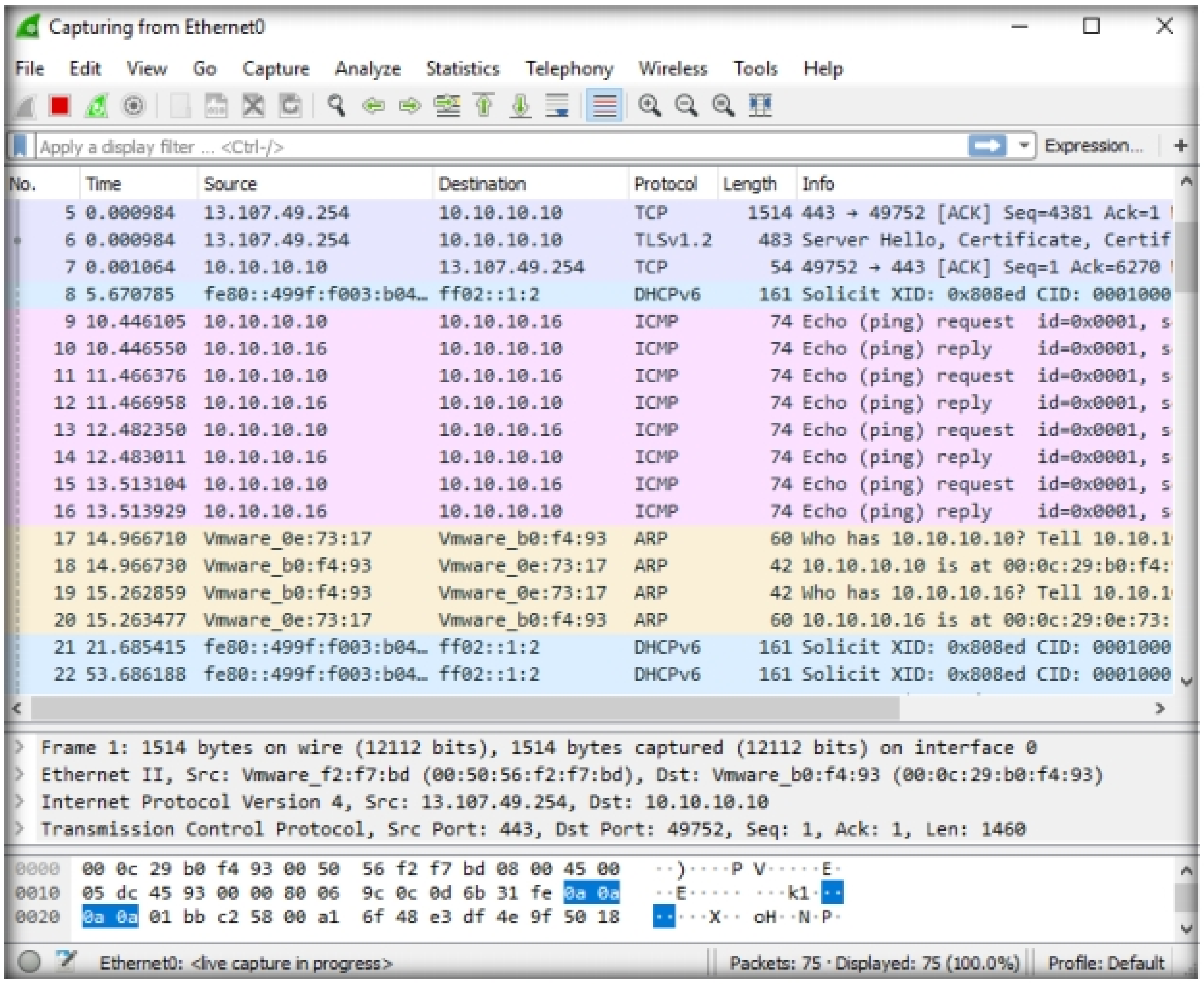
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.10.16

Pinging 10.10.10.16 with 32 bytes of data:
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>
```

Figure 3.1.6: Sending ICMP requests to Windows Server 2016 virtual machine

TASK 1.4

Analyze the TTL Value

13. Observe the packets captured by **Wireshark**.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

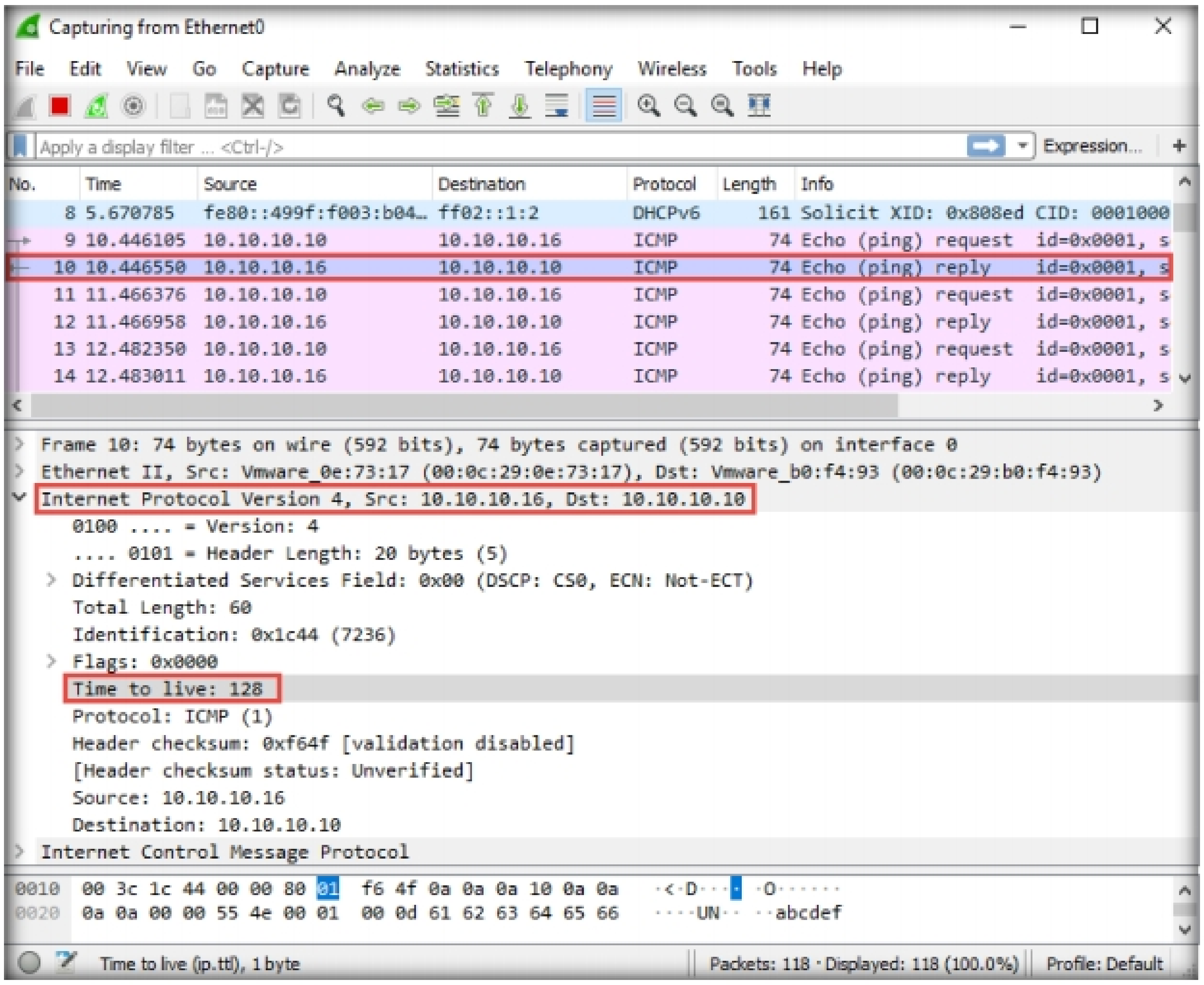
```
No.  Time        Source                     Destination       Protocol  Length Info
   5 0.000984    13.107.49.254              10.10.10.10       TCP         1514 443 → 49752 [ACK] Seq=4381 Ack=1
   6 0.000984    13.107.49.254              10.10.10.10       TLSv1.2      483 Server Hello, Certificate, Certif
   7 0.001064    10.10.10.10                13.107.49.254     TCP           54 49752 → 443 [ACK] Seq=1 Ack=6270
   8 5.670785    fe80::499f:f003:b04…       ff02::1:2         DHCPv6       161 Solicit XID: 0x808ed CID: 0001000
   9 10.446105   10.10.10.10                10.10.10.16       ICMP          74 Echo (ping) request  id=0x0001, s
  10 10.446550   10.10.10.16                10.10.10.10       ICMP          74 Echo (ping) reply    id=0x0001, s
  11 11.466376   10.10.10.10                10.10.10.16       ICMP          74 Echo (ping) request  id=0x0001, s
  12 11.466958   10.10.10.16                10.10.10.10       ICMP          74 Echo (ping) reply    id=0x0001, s
  13 12.482350   10.10.10.10                10.10.10.16       ICMP          74 Echo (ping) request  id=0x0001, s
  14 12.483011   10.10.10.16                10.10.10.10       ICMP          74 Echo (ping) reply    id=0x0001, s
  15 13.513104   10.10.10.10                10.10.10.16       ICMP          74 Echo (ping) request  id=0x0001, s
  16 13.513929   10.10.10.16                10.10.10.10       ICMP          74 Echo (ping) reply    id=0x0001, s
  17 14.966710   Vmware_0e:73:17            Vmware_b0:f4:93   ARP           60 Who has 10.10.10.10? Tell 10.10.1
  18 14.966730   Vmware_b0:f4:93            Vmware_0e:73:17   ARP           42 10.10.10.10 is at 00:0c:29:b0:f4:
  19 15.262859   Vmware_b0:f4:93            Vmware_0e:73:17   ARP           42 Who has 10.10.10.16? Tell 10.10.1
  20 15.263477   Vmware_0e:73:17            Vmware_b0:f4:93   ARP           60 10.10.10.16 is at 00:0c:29:0e:73:
  21 21.685415   fe80::499f:f003:b04…       ff02::1:2         DHCPv6       161 Solicit XID: 0x808ed CID: 0001000
  22 53.686188   fe80::499f:f003:b04…       ff02::1:2         DHCPv6       161 Solicit XID: 0x808ed CID: 0001000

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Vmware_f2:f7:bd (00:50:56:f2:f7:bd), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)
> Internet Protocol Version 4, Src: 13.107.49.254, Dst: 10.10.10.10
> Transmission Control Protocol, Src Port: 443, Dst Port: 49752, Seq: 1, Ack: 1, Len: 1460

0000  00 0c 29 b0 f4 93 00 50  56 f2 f7 bd 08 00 45 00   ··)····P V·····E·
0010  05 dc 45 93 00 00 80 06  9c 0c 0d 6b 31 fe 0a 0a   ··E·····  ···k1···
0020  0a 0a 01 bb c2 58 00 a1  6f 48 e3 df 4e 9f 50 18   ·····X··  oH··N·P·

Ethernet0: <live capture in progress>    Packets: 75 · Displayed: 75 (100.0%)    Profile: Default
```

Figure 3.1.7: Packets Captured by Wireshark

14. Choose any packet of the ICMP reply from the **Windows Server 2016** (**10.10.10.16**) to **Windows 10** (**10.10.10.10**) virtual machines and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

Note: The IP address may vary in your lab environment.

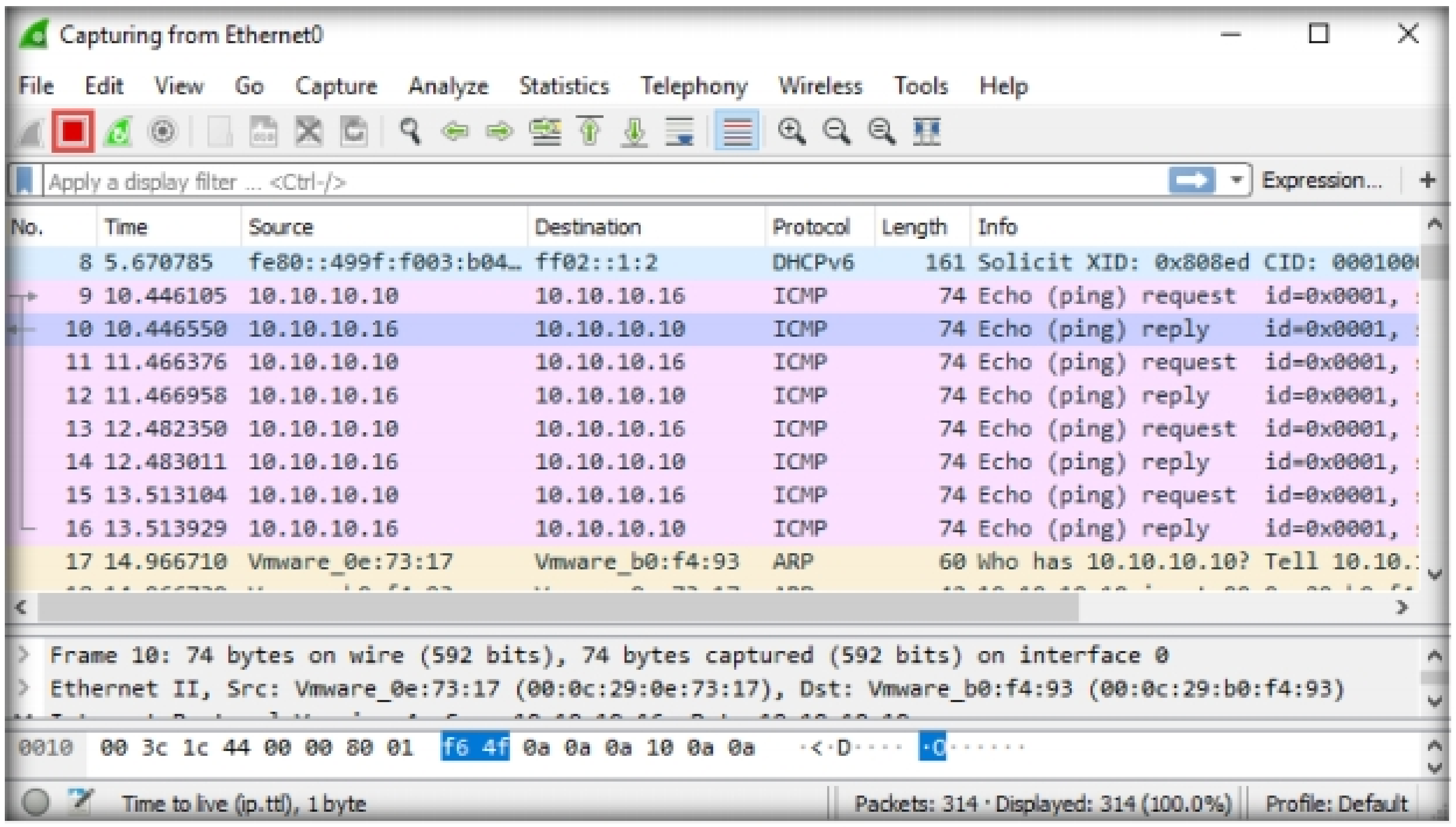
15. The TTL value is recorded as **128**, which means that the ICMP reply possibly came from a Windows-based machine.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Time to live (ip.ttl), 1 byte
Packets: 118 · Displayed: 118 (100.0%)
Profile: Default

```
No.  Time       Source                 Destination  Protocol Length Info
   8 5.670785   fe80::499f:f003:b04…   ff02::1:2    DHCPv6     161 Solicit XID: 0x808ed CID: 0001000
   9 10.446105  10.10.10.10            10.10.10.16  ICMP        74 Echo (ping) request  id=0x0001, s
  10 10.446550  10.10.10.16            10.10.10.10  ICMP        74 Echo (ping) reply    id=0x0001, s
  11 11.466376  10.10.10.10            10.10.10.16  ICMP        74 Echo (ping) request  id=0x0001, s
  12 11.466958  10.10.10.16            10.10.10.10  ICMP        74 Echo (ping) reply    id=0x0001, s
  13 12.482350  10.10.10.10            10.10.10.16  ICMP        74 Echo (ping) request  id=0x0001, s
  14 12.483011  10.10.10.16            10.10.10.10  ICMP        74 Echo (ping) reply    id=0x0001, s

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_0e:73:17 (00:0c:29:0e:73:17), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)
v Internet Protocol Version 4, Src: 10.10.10.16, Dst: 10.10.10.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x1c44 (7236)
  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0xf64f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.16
    Destination: 10.10.10.10
> Internet Control Message Protocol

0010  00 3c 1c 44 00 00 80 01  f6 4f 0a 0a 0a 10 0a 0a   ·<·D····  ·O······
0020  0a 0a 00 00 55 4e 00 01  00 0d 61 62 63 64 65 66   ····UN··  ··abcdef
```

Figure 3.1.8: TTL value detected by Wireshark for Windows Server 2016 virtual machine

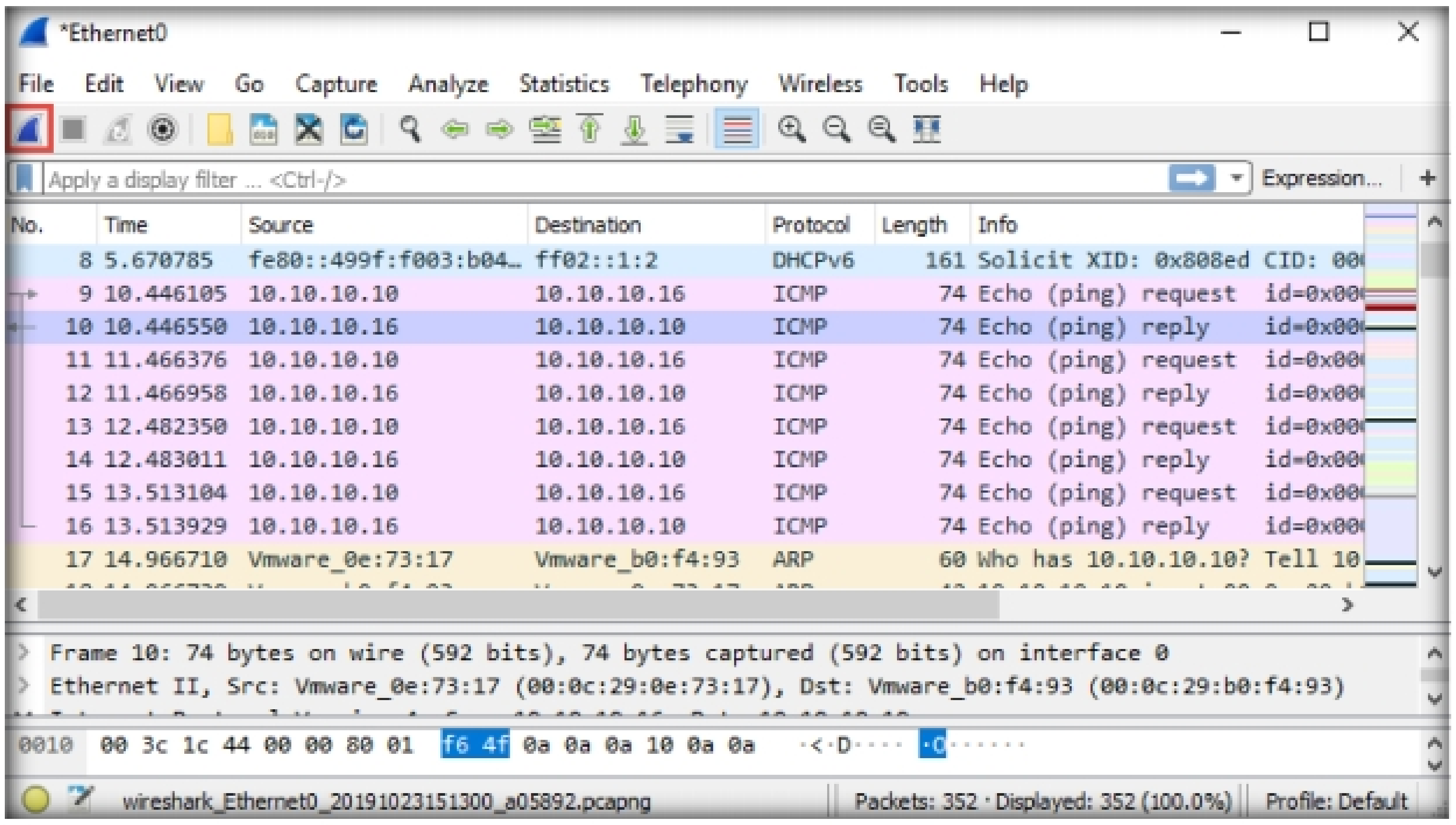
16. Now, stop the capture in the **Wireshark** window by clicking on the **Stop** (■) button.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Time to live (ip.ttl), 1 byte
Packets: 314 · Displayed: 314 (100.0%)
Profile: Default

```
No.  Time       Source                 Destination      Protocol Length Info
   8 5.670785   fe80::499f:f003:b04…   ff02::1:2        DHCPv6     161 Solicit XID: 0x808ed CID: 000100
   9 10.446105  10.10.10.10            10.10.10.16      ICMP        74 Echo (ping) request  id=0x0001,
  10 10.446550  10.10.10.16            10.10.10.10      ICMP        74 Echo (ping) reply    id=0x0001,
  11 11.466376  10.10.10.10            10.10.10.16      ICMP        74 Echo (ping) request  id=0x0001,
  12 11.466958  10.10.10.16            10.10.10.10      ICMP        74 Echo (ping) reply    id=0x0001,
  13 12.482350  10.10.10.10            10.10.10.16      ICMP        74 Echo (ping) request  id=0x0001,
  14 12.483011  10.10.10.16            10.10.10.10      ICMP        74 Echo (ping) reply    id=0x0001,
  15 13.513104  10.10.10.10            10.10.10.16      ICMP        74 Echo (ping) request  id=0x0001,
  16 13.513929  10.10.10.16            10.10.10.10      ICMP        74 Echo (ping) reply    id=0x0001,
  17 14.966710  Vmware_0e:73:17        Vmware_b0:f4:93  ARP         60 Who has 10.10.10.10? Tell 10.10.

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_0e:73:17 (00:0c:29:0e:73:17), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)

0010  00 3c 1c 44 00 00 80 01  f6 4f 0a 0a 0a 10 0a 0a   ·<·D····  ·O······
```

Figure 3.1.9: Stop Live Capture in Wireshark

17. Now, click the **Start capturing packets** ( ) button. If an **Unsaved packets...** pop-up appears, click **Continue without Saving**.



*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time       Source                 Destination     Protocol  Length Info
    8 5.670785   fe80::499f:f003:b04…   ff02::1:2       DHCPv6       161 Solicit XID: 0x808ed CID: 00
    9 10.446105  10.10.10.10            10.10.10.16     ICMP          74 Echo (ping) request  id=0x00
   10 10.446550  10.10.10.16            10.10.10.10     ICMP          74 Echo (ping) reply    id=0x00
   11 11.466376  10.10.10.10            10.10.10.16     ICMP          74 Echo (ping) request  id=0x00
   12 11.466958  10.10.10.16            10.10.10.10     ICMP          74 Echo (ping) reply    id=0x00
   13 12.482350  10.10.10.10            10.10.10.16     ICMP          74 Echo (ping) request  id=0x00
   14 12.483011  10.10.10.16            10.10.10.10     ICMP          74 Echo (ping) reply    id=0x00
   15 13.513104  10.10.10.10            10.10.10.16     ICMP          74 Echo (ping) request  id=0x00
   16 13.513929  10.10.10.16            10.10.10.10     ICMP          74 Echo (ping) reply    id=0x00
   17 14.966710  Vmware_0e:73:17        Vmware_b0:f4:93 ARP           60 Who has 10.10.10.10? Tell 10

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_0e:73:17 (00:0c:29:0e:73:17), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)

0010  00 3c 1c 44 00 00 80 01  f6 4f 0a 0a 0a 10 0a 0a   ·<·D···· ·O······

wireshark_Ethernet0_20191023151300_a05892.pcapng    Packets: 352 · Displayed: 352 (100.0%)    Profile: Default
```

Figure 3.1.10: Start Live Capture in Wireshark

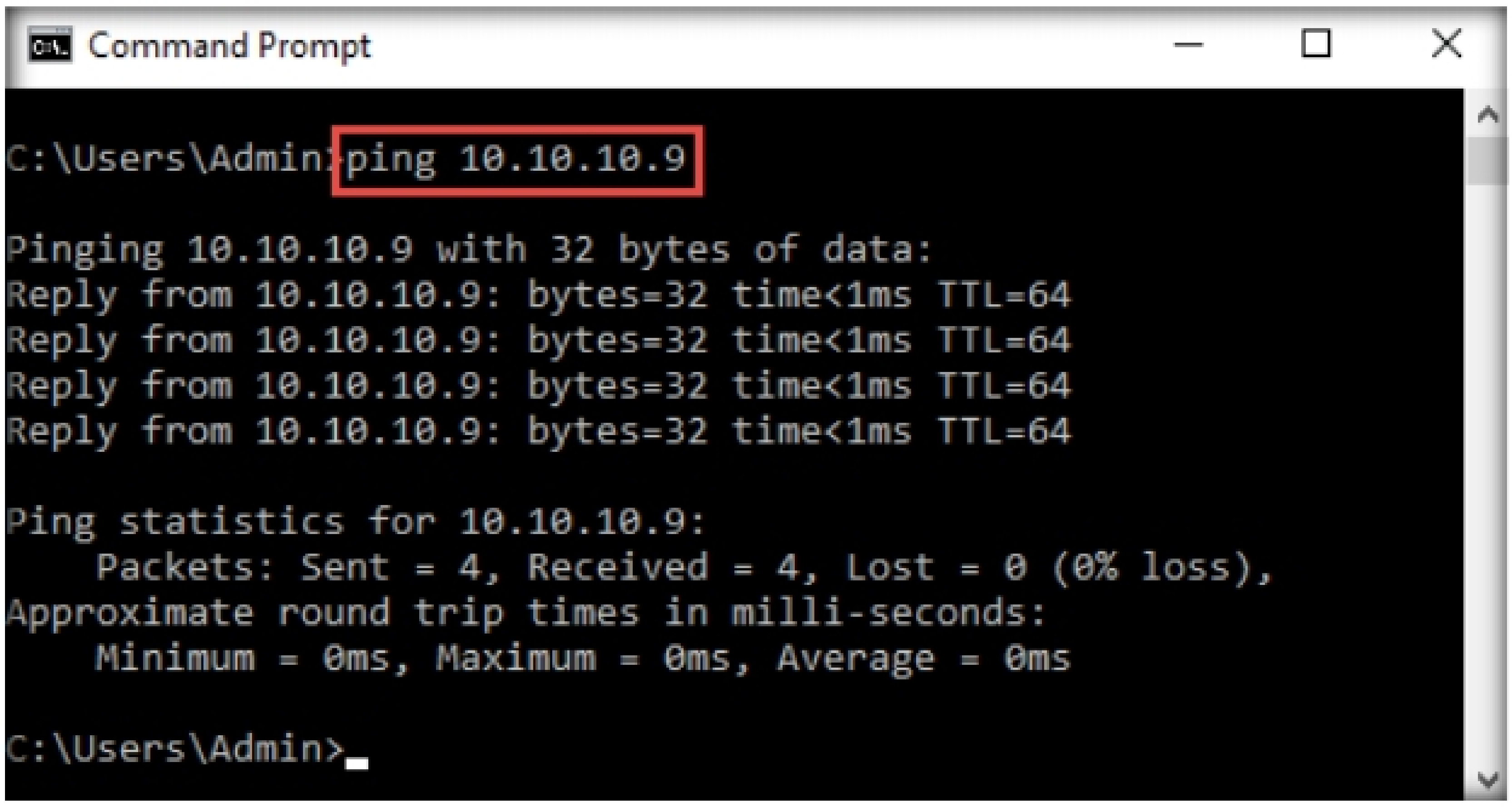
18. Wireshark will start capturing the new packets.

TASK 1.5

Perform Ping on Target Machine (Linux)

19. In the **Command Prompt** window, type **ping 10.10.10.9** and press **Enter**.

Note: **10.10.10.9** is the IP address of the **Ubuntu** virtual machine; this may vary in your lab environment.



```
C:\Users\Admin>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:
Reply from 10.10.10.9: bytes=32 time<1ms TTL=64
Reply from 10.10.10.9: bytes=32 time<1ms TTL=64
Reply from 10.10.10.9: bytes=32 time<1ms TTL=64
Reply from 10.10.10.9: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>
```

Figure 3.1.11: Sending ICMP requests to Ubuntu virtual machine

20. Observe the packets captured by **Wireshark**.

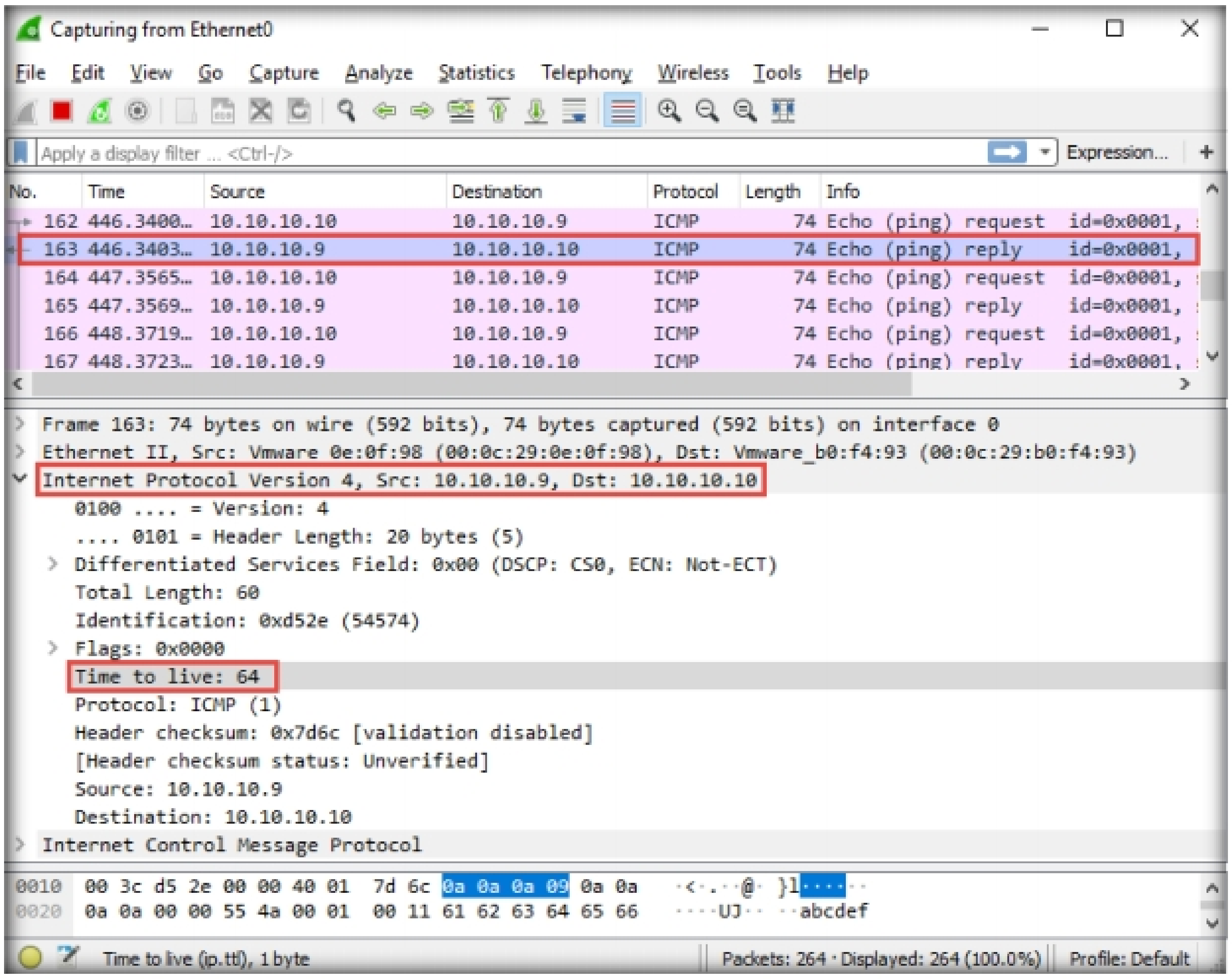
21. Choose any packet of ICMP reply from the **Ubuntu** (**10.10.10.9**) to **Windows 10** (**10.10.10.10**) virtual machine and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

TASK 1.6

Analyze the TTL Value

Note: The IP address may vary in your lab environment.

22. The TTL value is recorded as **64**, which means the ICMP reply possibly came from a Linux-based machine.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time          Source        Destination   Protocol  Length  Info
 162 446.3400…  10.10.10.10   10.10.10.9    ICMP        74 Echo (ping) request  id=0x0001,
 163 446.3403…  10.10.10.9    10.10.10.10   ICMP        74 Echo (ping) reply    id=0x0001,
 164 447.3565…  10.10.10.10   10.10.10.9    ICMP        74 Echo (ping) request  id=0x0001,
 165 447.3569…  10.10.10.9    10.10.10.10   ICMP        74 Echo (ping) reply    id=0x0001,
 166 448.3719…  10.10.10.10   10.10.10.9    ICMP        74 Echo (ping) request  id=0x0001,
 167 448.3723…  10.10.10.9    10.10.10.10   ICMP        74 Echo (ping) reply    id=0x0001,
```

```
> Frame 163: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_0e:0f:98 (00:0c:29:0e:0f:98), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)
v Internet Protocol Version 4, Src: 10.10.10.9, Dst: 10.10.10.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xd52e (54574)
  > Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x7d6c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.9
    Destination: 10.10.10.10
> Internet Control Message Protocol
```

```
0010  00 3c d5 2e 00 00 40 01  7d 6c 0a 0a 0a 09 0a 0a   ·<·.··@· }l······
0020  0a 0a 00 00 55 4a 00 01  00 11 61 62 63 64 65 66   ····UJ·· ··abcdef
```

Time to live (ip.ttl), 1 byte
Packets: 264 · Displayed: 264 (100.0%)
Profile: Default

Figure 3.1.12: Time-to-Live value detected by Wireshark for Linux machine

23. Stop the capture in the **Wireshark** window by clicking on the **Stop** button.

24. This concludes the demonstration of identifying the OS of the target system using Wireshark.

25. Close all open windows and document all the acquired information.

26. Turn off the **Ubuntu** virtual machine.

TASK 2

Perform OS Discovery using Nmap Script Engine (NSE)

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

Note: Before beginning this lab, ensure that the **Windows 10** and **Windows Server 2016** virtual machines are turned on.

1. In the **Windows 10** virtual machine, click on the **Start** menu and launch **Nmap - Zenmap GUI** from the applications.

TASK 2.1

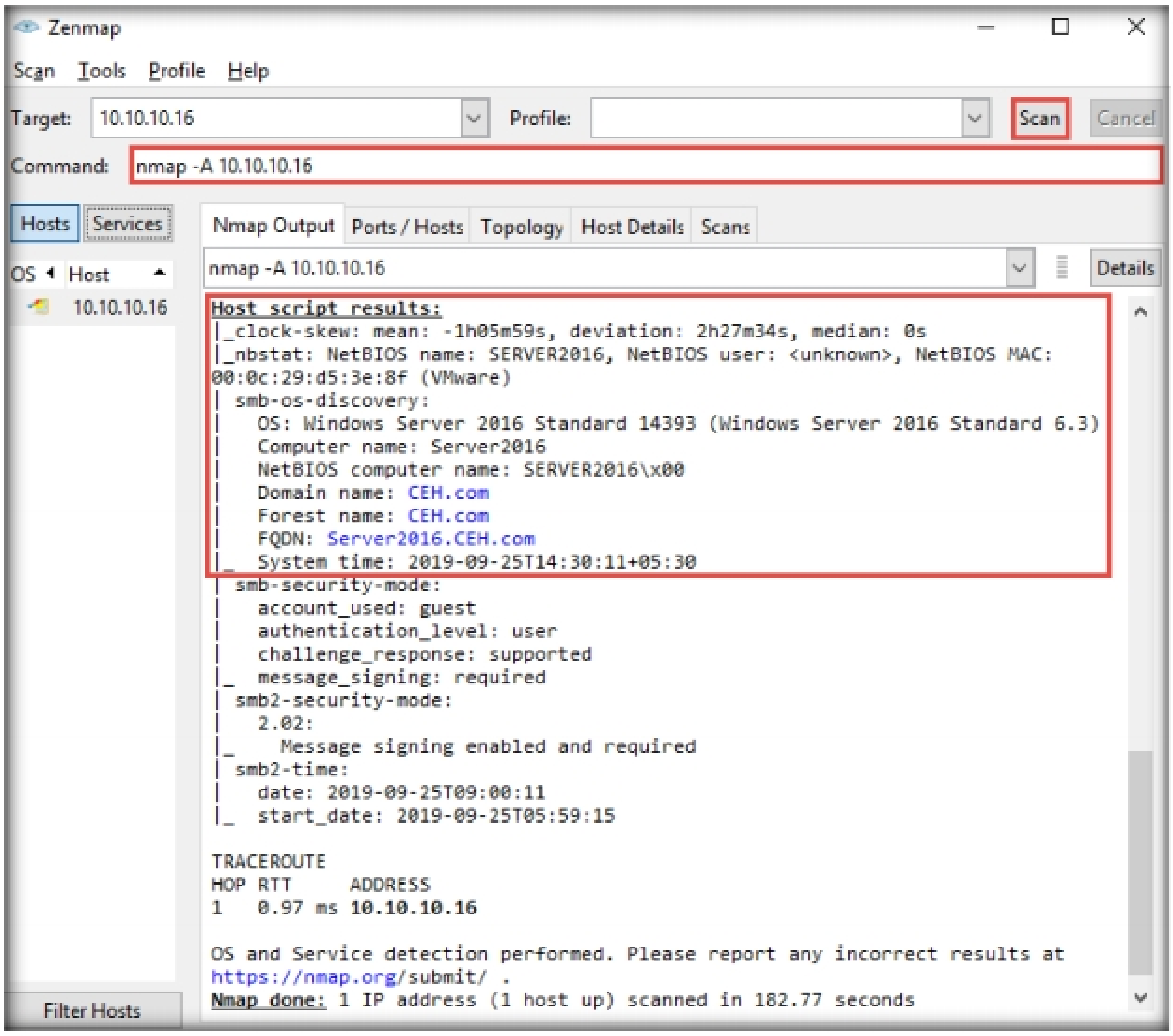
Perform OS Discovery Using -A Parameter (Aggressive Scan)

2. The **Zenmap** GUI appears. In the **Command** field, type the command **nmap -A <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-A**: to perform an aggressive scan.

3. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.



Target: 10.10.10.16

Profile:

Command: nmap -A 10.10.10.16

10.10.10.16

```
nmap -A 10.10.10.16
Host script results:
|_clock-skew: mean: -1h05m59s, deviation: 2h27m34s, median: 0s
|_nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:d5:3e:8f (VMware)
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Server2016
|   NetBIOS computer name: SERVER2016\x00
|   Domain name: CEH.com
|   Forest name: CEH.com
|   FQDN: Server2016.CEH.com
|_  System time: 2019-09-25T14:30:11+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-09-25T09:00:11
|_  start_date: 2019-09-25T05:59:15

TRACEROUTE
HOP RTT     ADDRESS
1   0.97 ms 10.10.10.16

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.77 seconds
```

Figure 3.2.1: Zenmap scan results for -A parameter

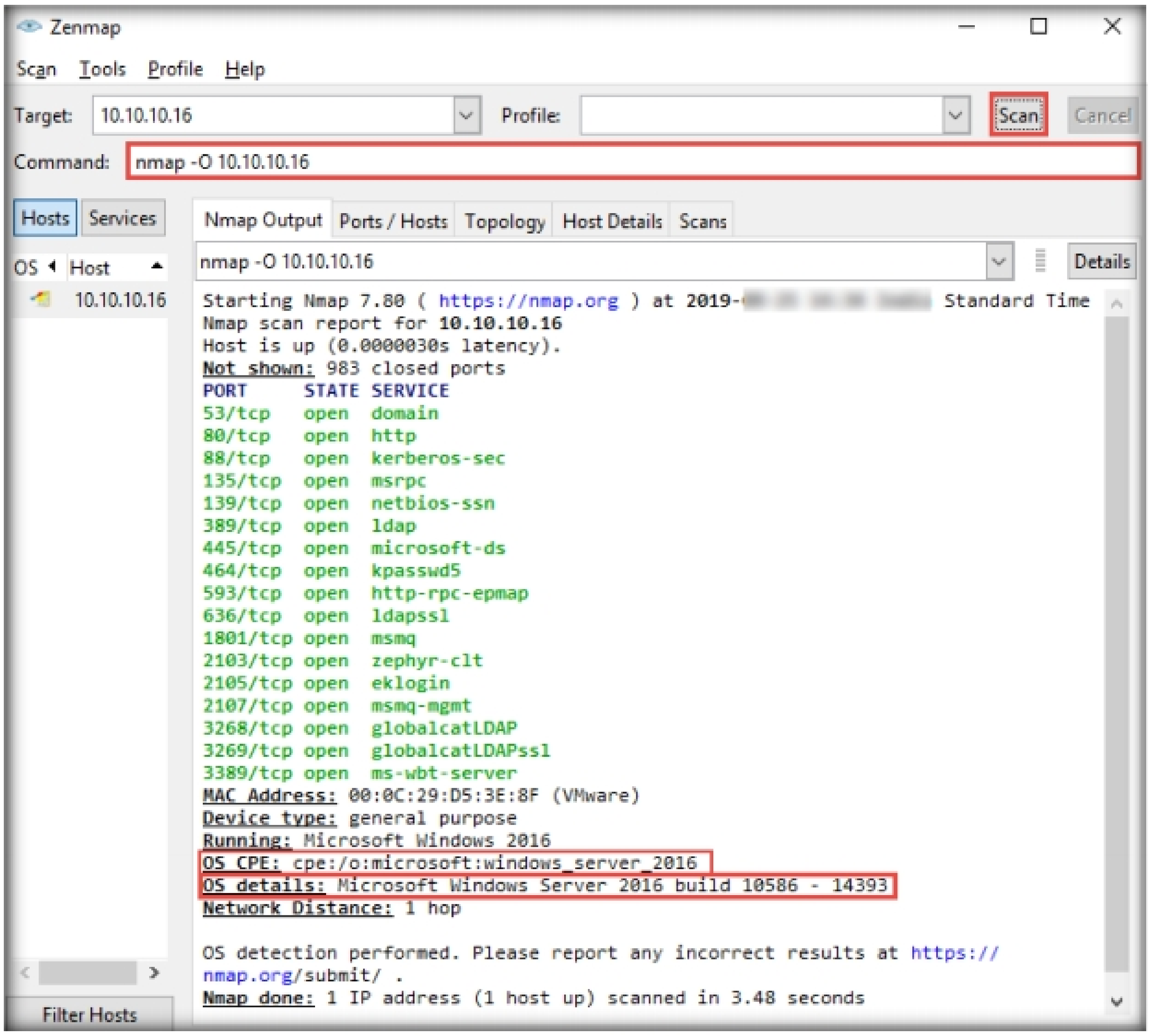
TASK 2.2

Perform OS Discovery Using -O Parameter

4. In the **Command** field, type the command **nmap -O <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-O**: performs the OS discovery.

5. The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.



Zenmap
Scan
Tools
Profile
Help
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
10.10.10.16
Details
Filter Hosts

Target: 10.10.10.16

Command: nmap -O 10.10.10.16

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-[redacted] Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.0000030s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.48 seconds
```

Figure 3.2.2: Zenmap scan results for -O parameter

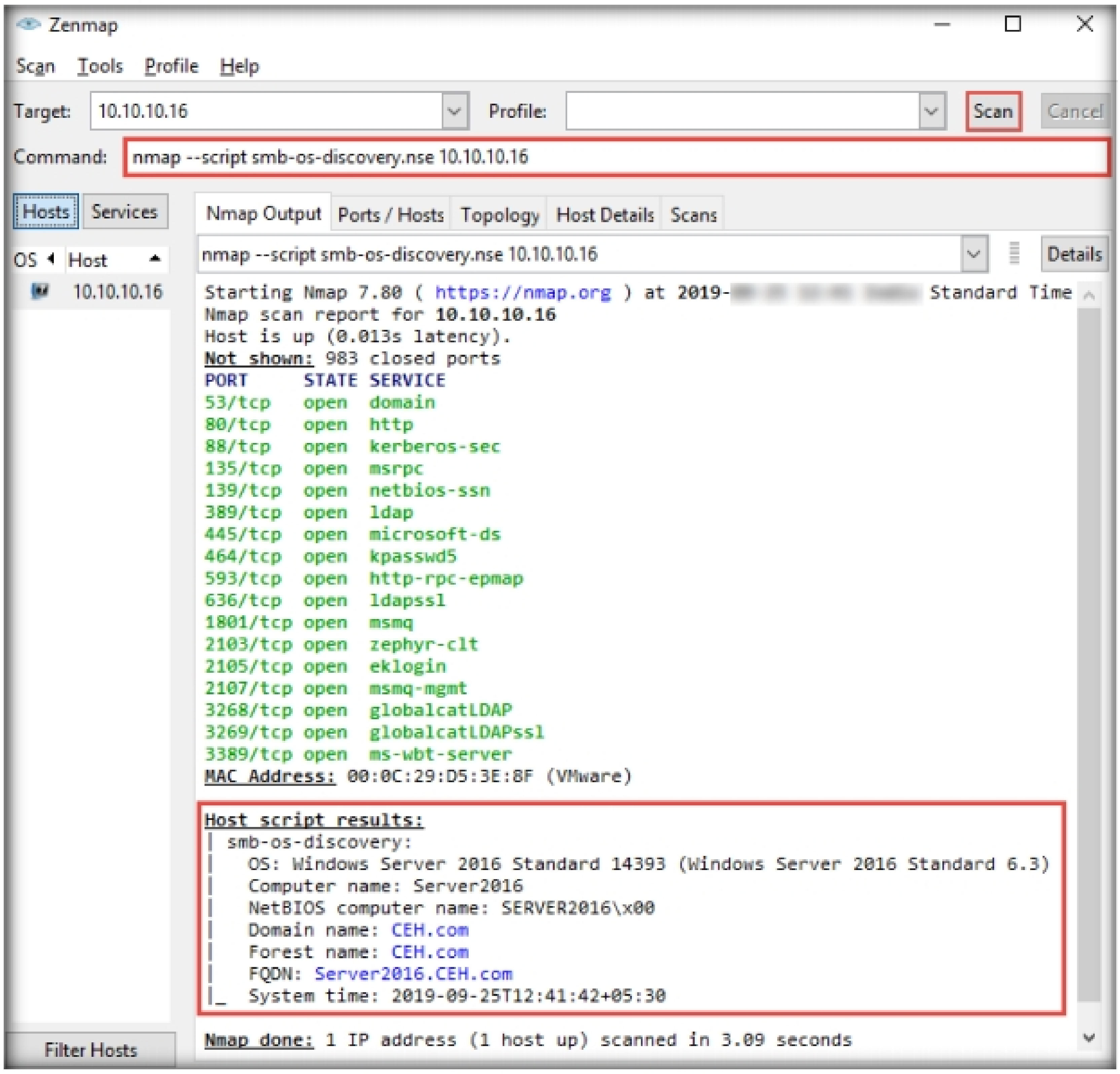
TASK 2.3

Perform OS Discovery Using NSE

6. In the **Command** field, type the command **nmap --script smb-os-discovery.nse <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **--script**: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

7. The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.



Target: 10.10.10.16

Command: nmap --script smb-os-discovery.nse 10.10.10.16

```
nmap --script smb-os-discovery.nse 10.10.10.16
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-[redacted] Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.013s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Server2016
|   NetBIOS computer name: SERVER2016\x00
|   Domain name: CEH.com
|   Forest name: CEH.com
|   FQDN: Server2016.CEH.com
|_  System time: 2019-09-25T12:41:42+05:30

Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds
```

Figure 3.2.3: Zenmap scan results for NSE

8. This concludes the demonstration of discovering the OS running on the target system using Nmap.

9. Close all open windows and document all the acquired information.

TASK 3

Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Here, we will use the Unicornscan tool to perform OS discovery on the target system.

1. Before beginning this lab, turn on the **Parrot Security** and **Ubuntu** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is also running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

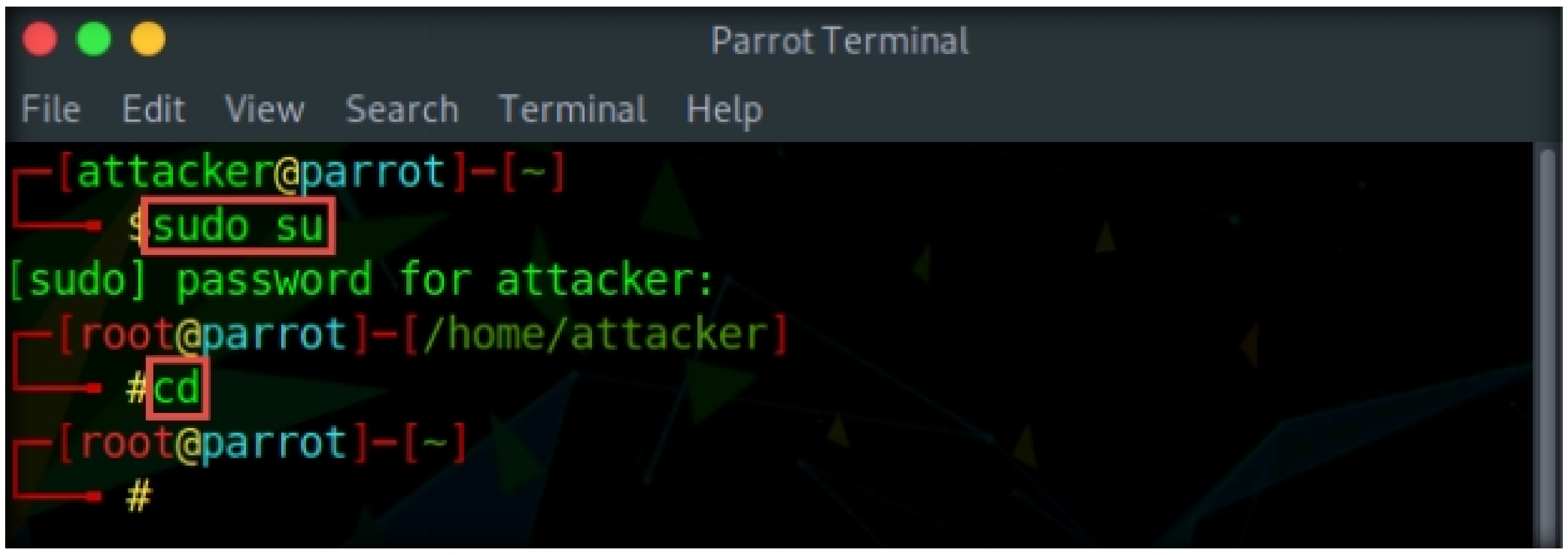
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

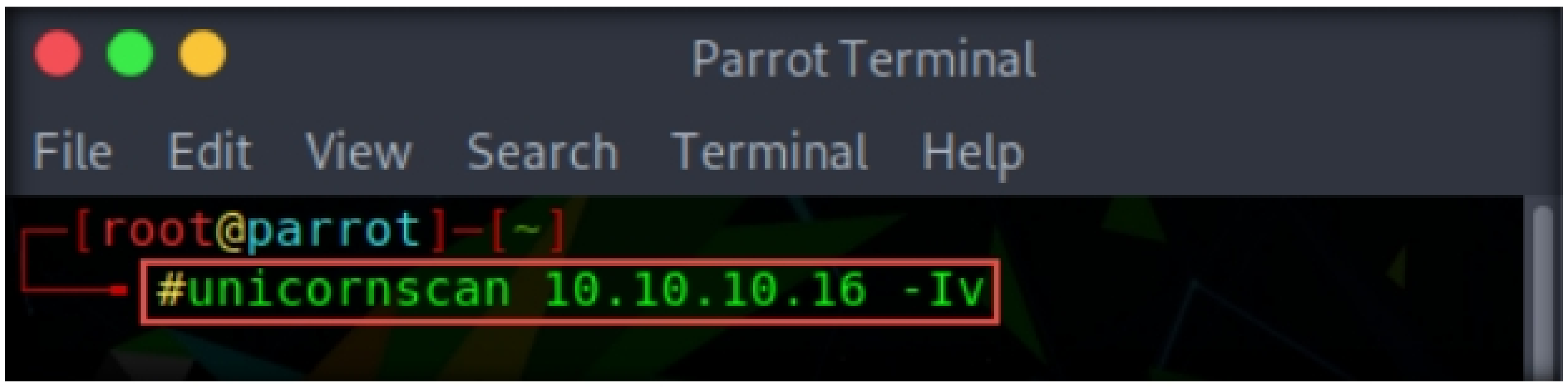
Figure 3.3.1: Running the programs as a root user

TASK 3.1

Perform OS Discovery on Windows-based Machine

7. In the terminal window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-I** specifies an immediate mode and **v** specifies a verbose mode.

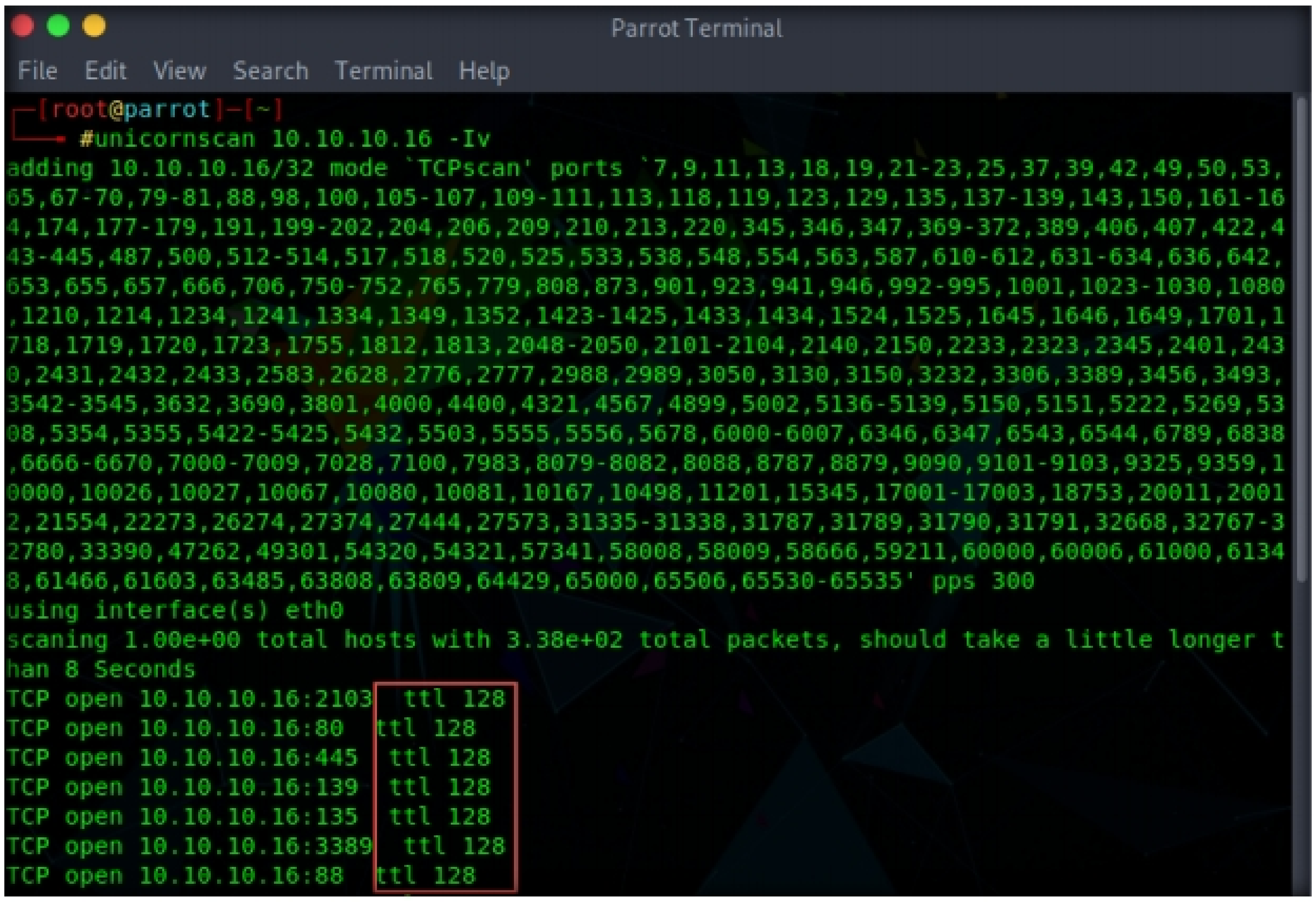


```
┌─[root@parrot]─[~]
└──╼ #unicornscan 10.10.10.16 -Iv
```

Figure 3.3.2: Unicornscan OS discovery command

8. The scan results appear, displaying the open TCP ports along with the obtained TTL value of **128**. As shown in the screenshot, the **ttl** values acquired after the scan are **128**; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

Note: Here, the target machine is **Windows Server 2016** (10.10.10.16).



```
┌─[root@parrot]─[~]
└──╼ #unicornscan 10.10.10.16 -Iv
adding 10.10.10.16/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,
65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-16
4,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,4
43-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,
653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080
,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1
718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,243
0,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,
3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,53
08,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838
,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,1
0000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2001
2,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-3
2780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,6134
8,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer t
han 8 Seconds
TCP open 10.10.10.16:2103  ttl 128
TCP open 10.10.10.16:80  ttl 128
TCP open 10.10.10.16:445  ttl 128
TCP open 10.10.10.16:139  ttl 128
TCP open 10.10.10.16:135  ttl 128
TCP open 10.10.10.16:3389  ttl 128
TCP open 10.10.10.16:88  ttl 128
```

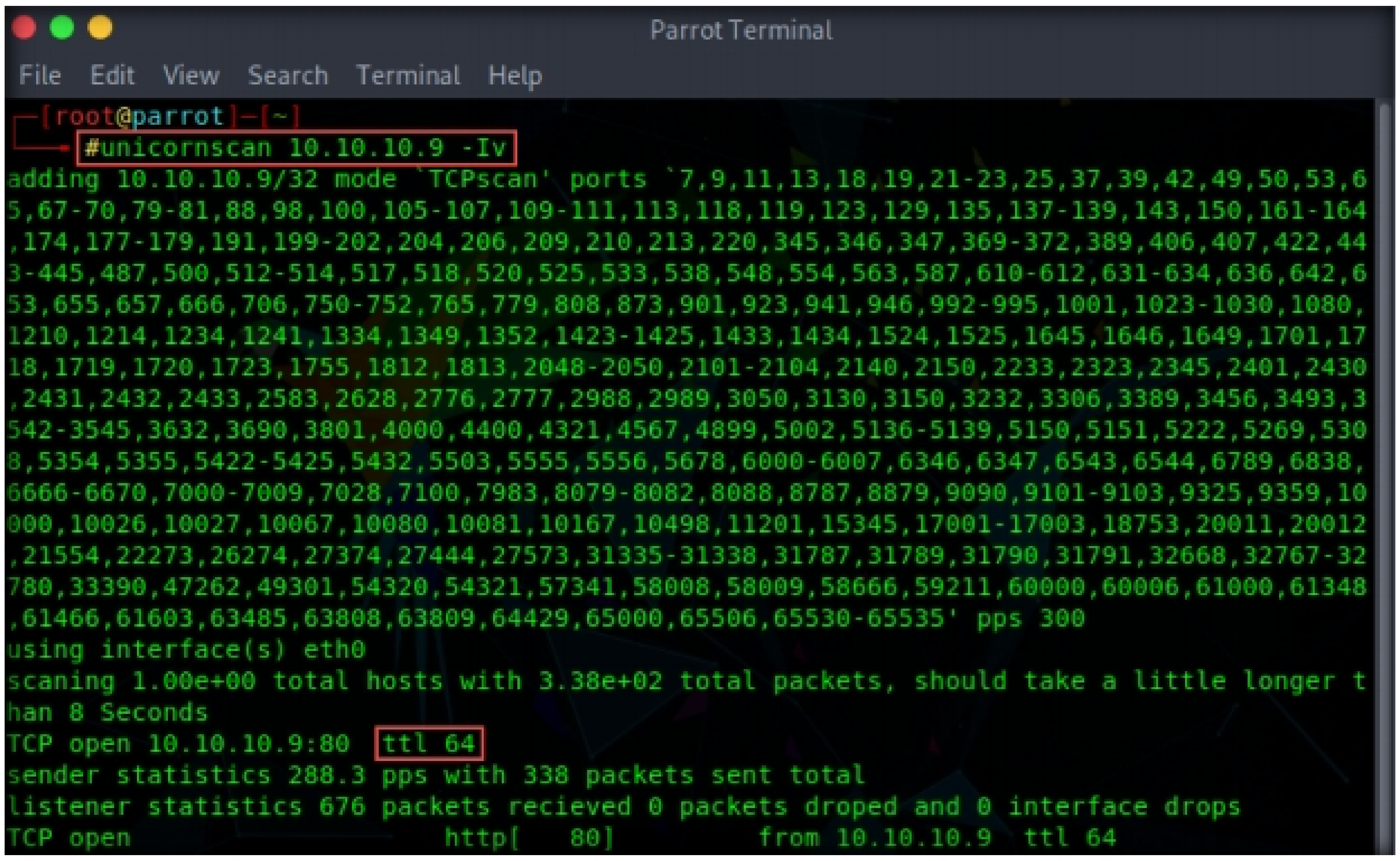
Figure 3.3.3: Unicornscan OS discovery command result Windows-based virtual machine

TASK 3.2

Perform OS Discovery on Linux-based Machine

9. In the **Parrot Terminal** window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Ubuntu [**10.10.10.9**]) and press **Enter**.

10. The scan results appear, displaying the open TCP ports along with a TTL value of **64**. As shown in the screenshot, the **ttl** value acquired after the scan is **64**; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali).



```
┌─[root@parrot]─[~]
└──╼ #unicornscan 10.10.10.9 -Iv
adding 10.10.10.9/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,6
5,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164
,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,44
3-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,6
53,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080,
1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,17
18,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2430
,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3
542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,530
8,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,
6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10
000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20012
,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-32
780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,61348
,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer t
han 8 Seconds
TCP open 10.10.10.9:80  ttl 64
sender statistics 288.3 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets droped and 0 interface drops
TCP open                    http[   80]         from 10.10.10.9  ttl 64
```

Figure 3.3.4: Unicornscan OS discovery command result for Linux-based virtual machine

11. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.

12. Close all open windows and document all the acquired information.

13. Turn off the **Windows 10**, **Parrot Security**, **Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

4

Scan beyond IDS and Firewall

Scanning beyond IDS and firewall is a process of sending intended packets to the target system in order to exploit IDS/firewall limitations.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 🕮 Workbook review

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques
- Create custom packets using Colasoft Packet Builder to scan beyond the IDS/firewall
- Create custom UDP and TCP packets using Hping3 to scan beyond the IDS/firewall
- Create custom packets using Nmap to scan beyond the IDS/firewall
- Browse anonymously using Proxy Switcher
- Browse anonymously using CyberGhost VPN

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Colasoft Packet Builder located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder**
- Proxy Switcher located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- CyberGhost VPN located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 45 Minutes

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation**: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UPD checksums to the intended target
- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions

- **Anonymizers**: Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

Lab Tasks

TASK 1

Scan beyond IDS/Firewall using various Evasion Techniques

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

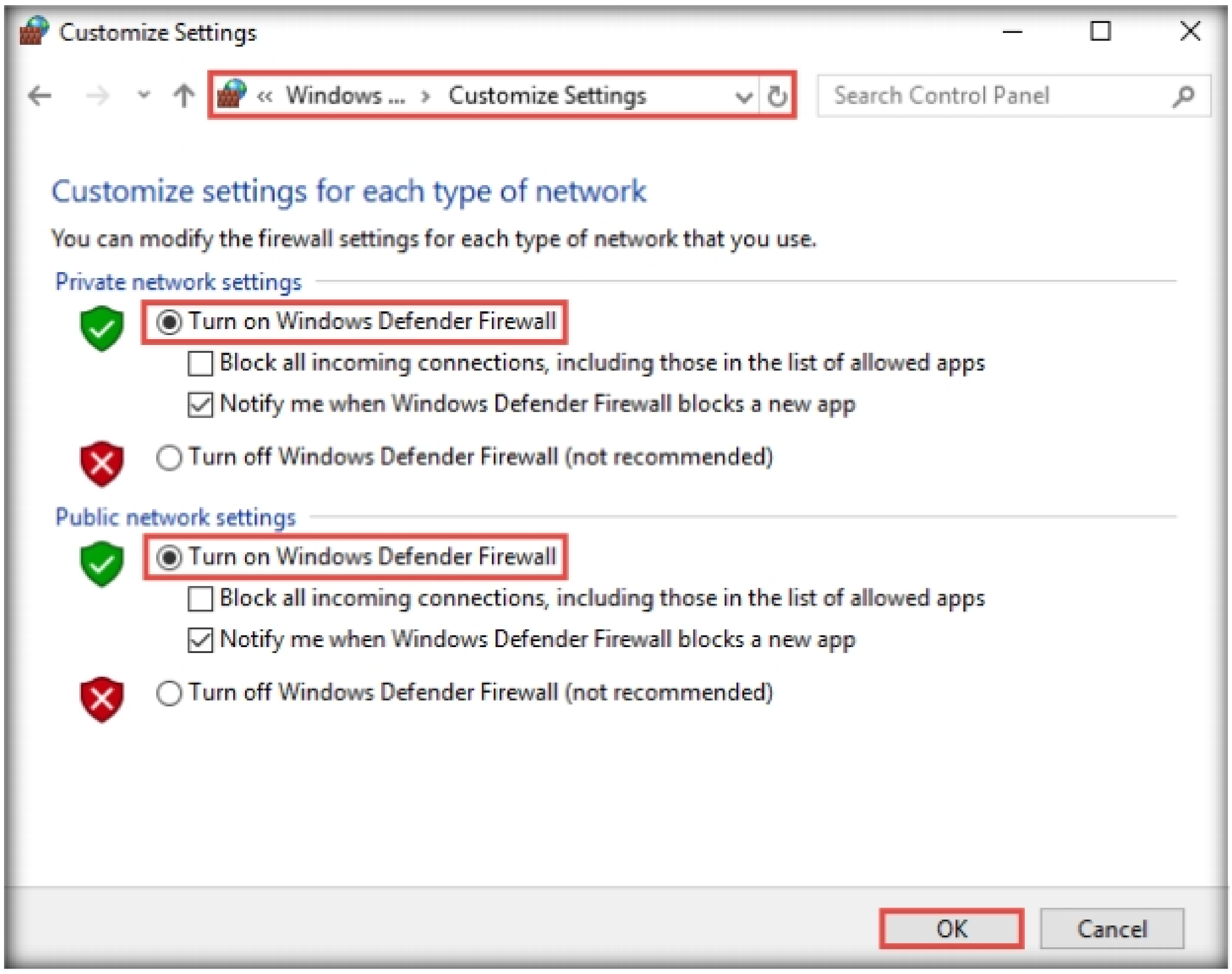
Note: In this lab, we are using the **Parrot Security** (10.10.10.13) virtual machine as a host machine and the **Windows 10** (10.10.10.10) virtual machine as a target machine.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin/Pa$$w0rd**.

TASK 1.1

Turn on Windows Defender Firewall

3. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Figure 4.1.1: Turn on Windows Defender Firewall

4. Click on the **Start** menu and launch **Wireshark** from the applications. Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet0**).

Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

Note: In this lab, the available interface might vary in your lab environment.

5. Now, switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

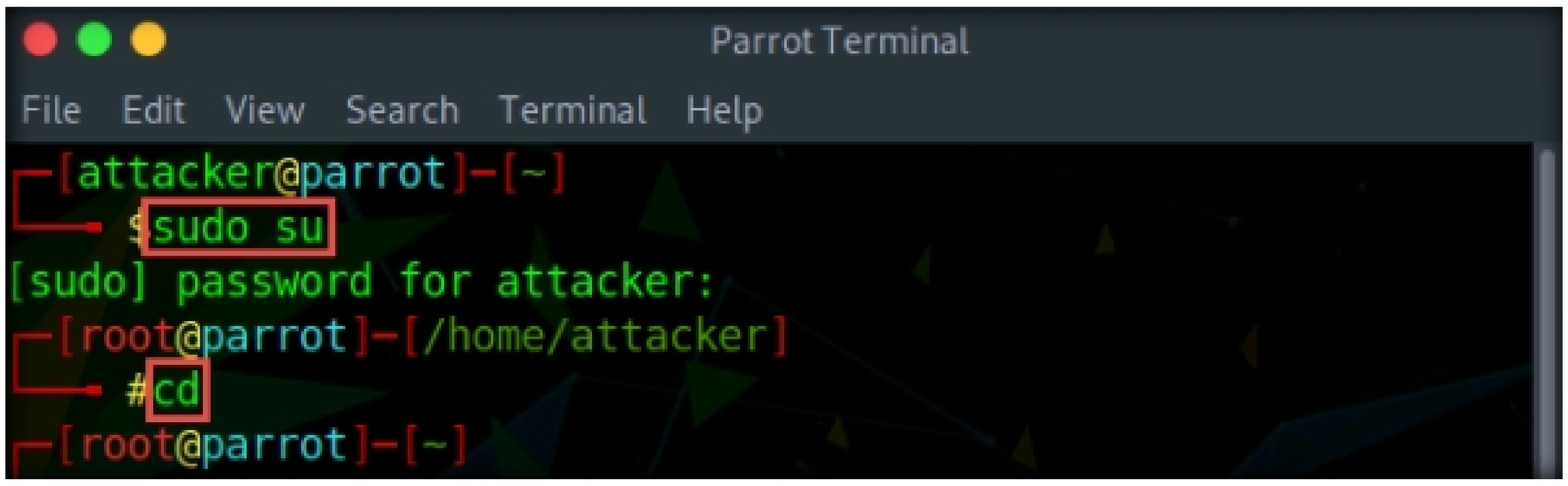
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
```

Figure 4.1.2: Running the programs as a root user

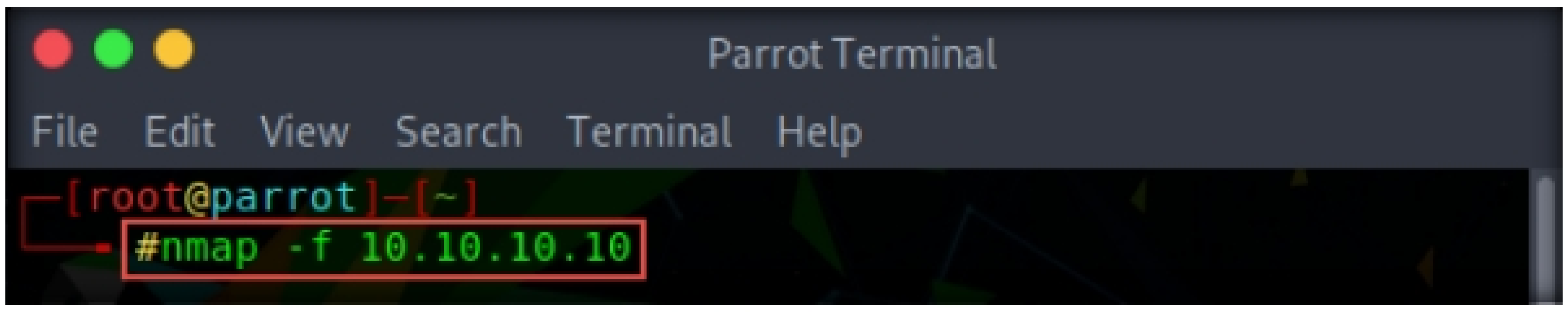
10. In the terminal window, type **nmap -f <Target IP Address>**, (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

TASK 1.2

Perform Packet Fragmentation

Note: **-f** switch is used to split the IP packet into tiny fragment packets.

Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

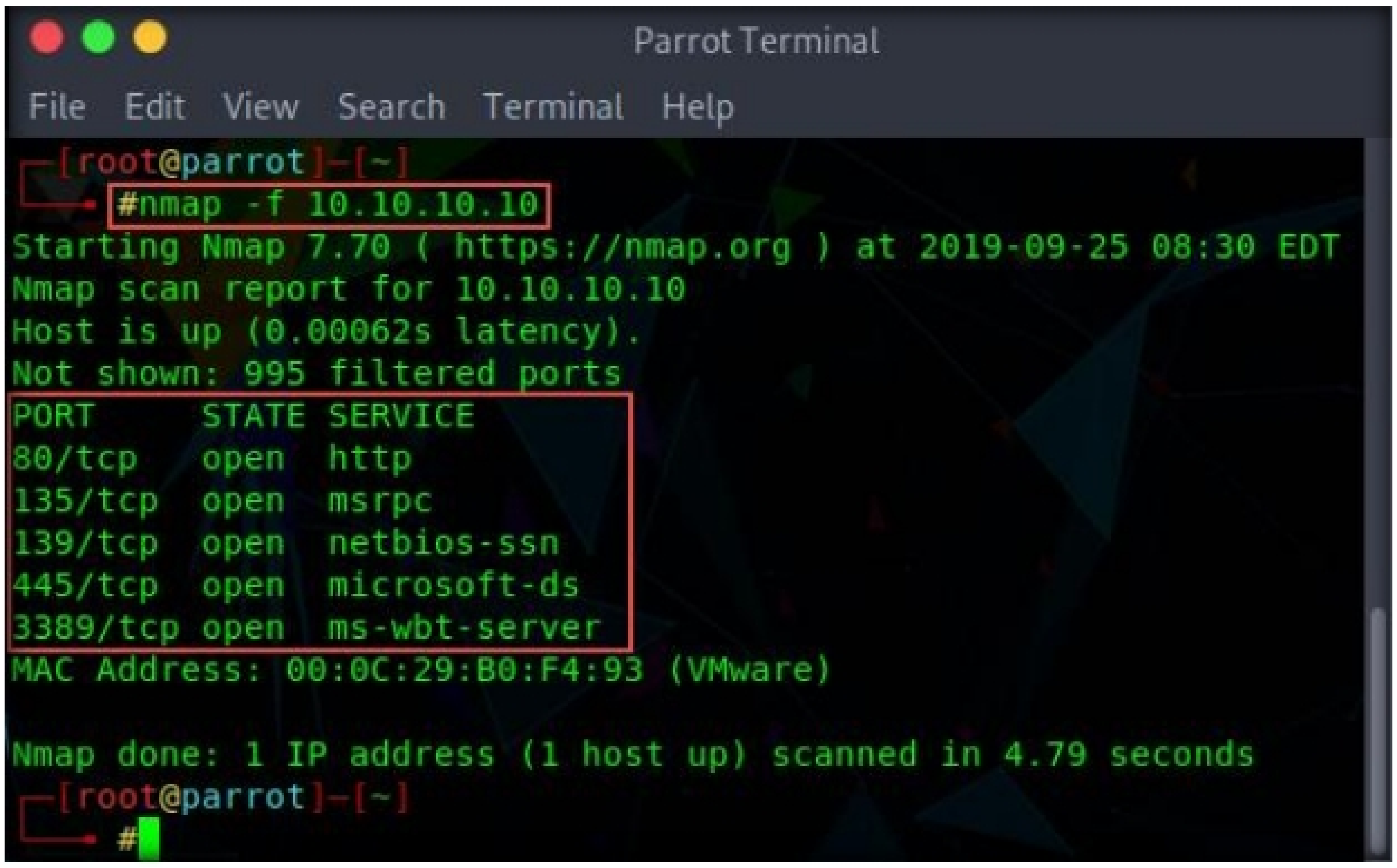


```
┌─[root@parrot]─[~]
└──╼ #nmap -f 10.10.10.10
```

Figure 4.1.3: Nmap fragment scan

11. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 10**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.



```
┌─[root@parrot]─[~]
└──╼ #nmap -f 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-25 08:30 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00062s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.1.4: Nmap fragment scan output

TASK 1.3

Perform Source Port Manipulation

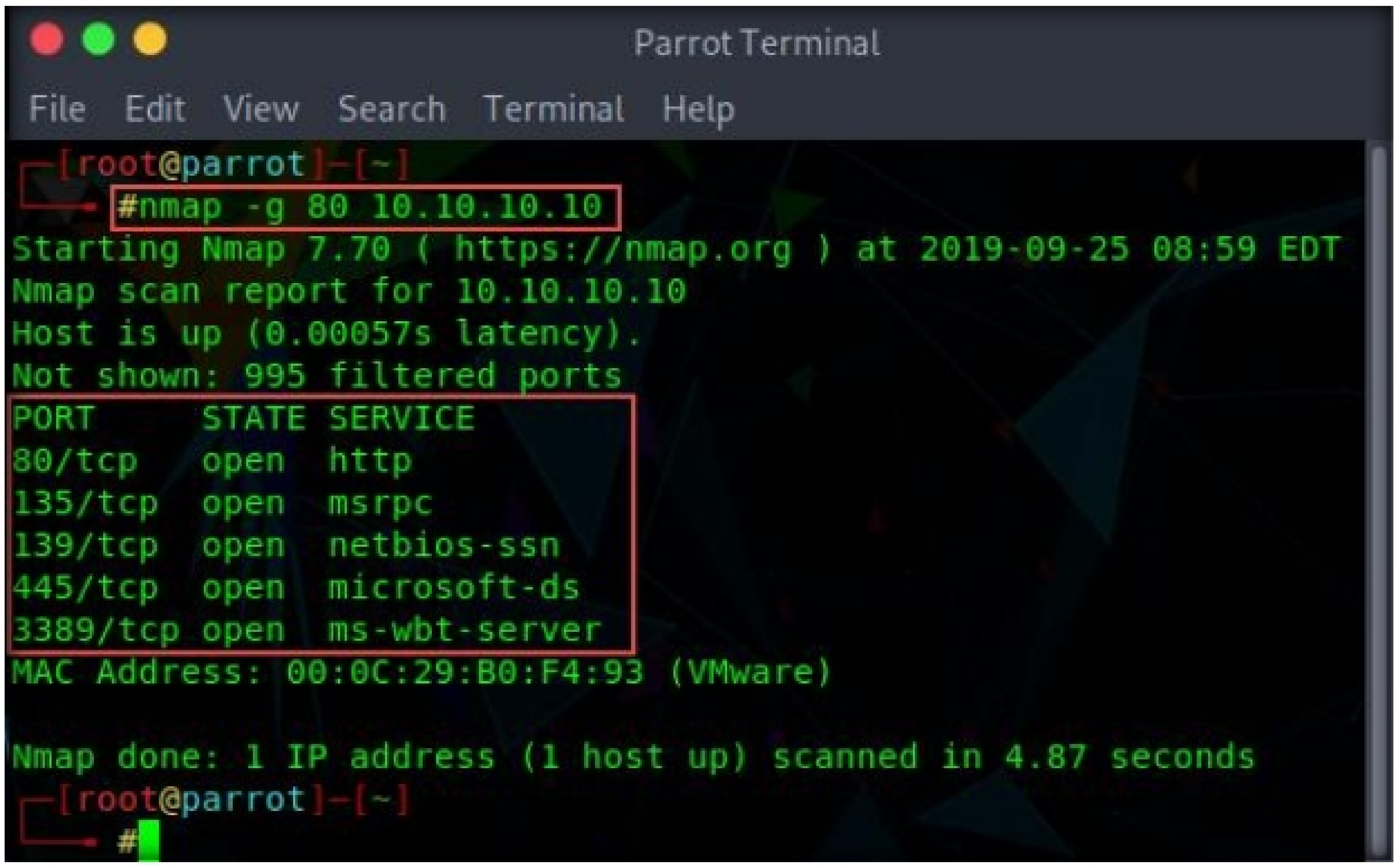
12. In the **Parrot Terminal** window, type **nmap -g 80 <Target IP Address>**, (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

Note: Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

13. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.



```
┌─[root@parrot]─[~]
└──╼ #nmap -g 80 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-25 08:59 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00057s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.1.5: Nmap source port manipulation scan output

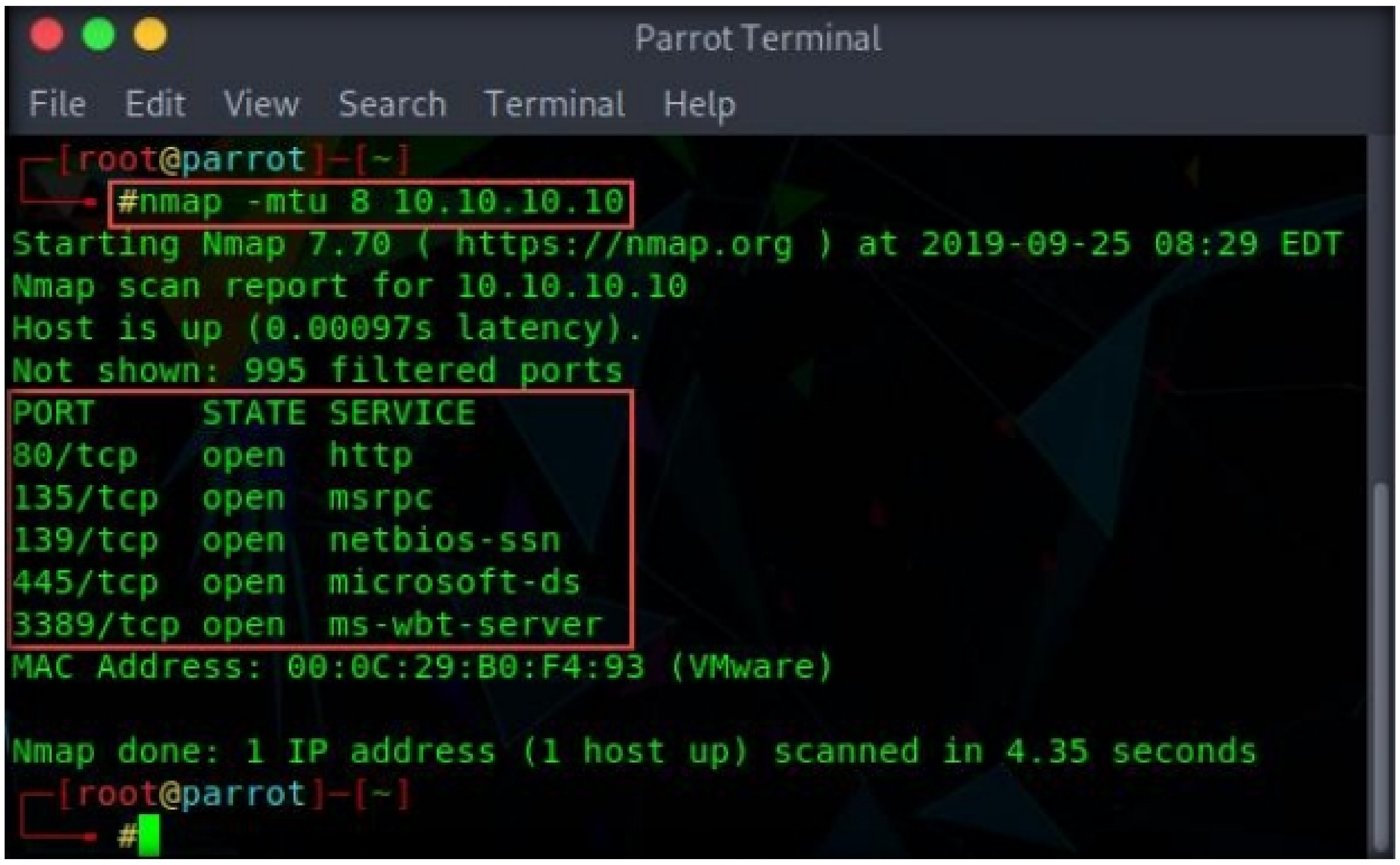
TASK 1.4

Perform Maximum Transmission Unit

14. Now, type **nmap -mtu 8 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.



```
┌─[root@parrot]─[~]
└──╼ #nmap -mtu 8 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-25 08:29 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00097s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.1.6: Nmap Maximum Transmission Unit scan

TASK 1.5

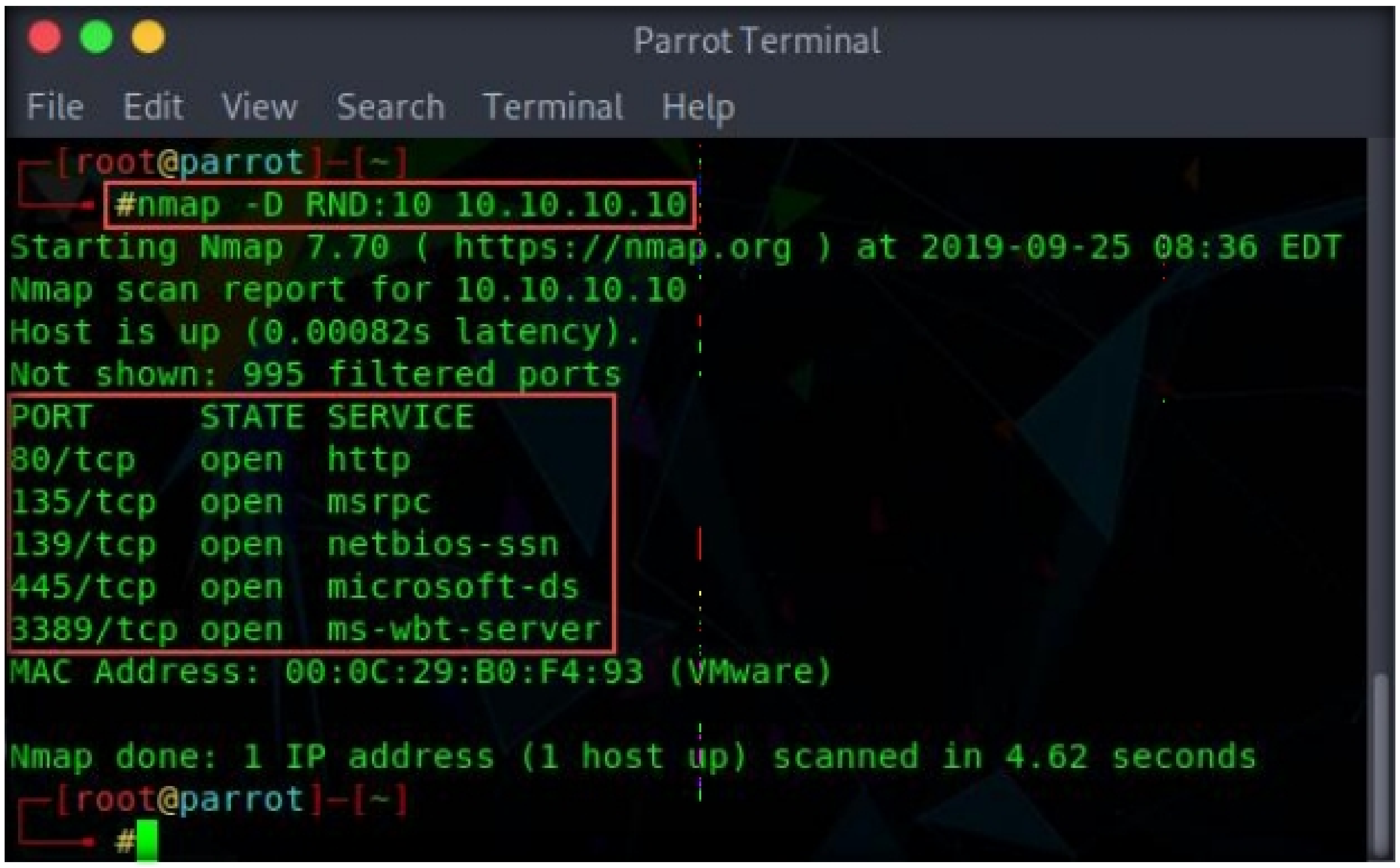
Perform IP Address Decoy

15. Now, type **nmap -D RND:10 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses.

Note: The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys.

By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

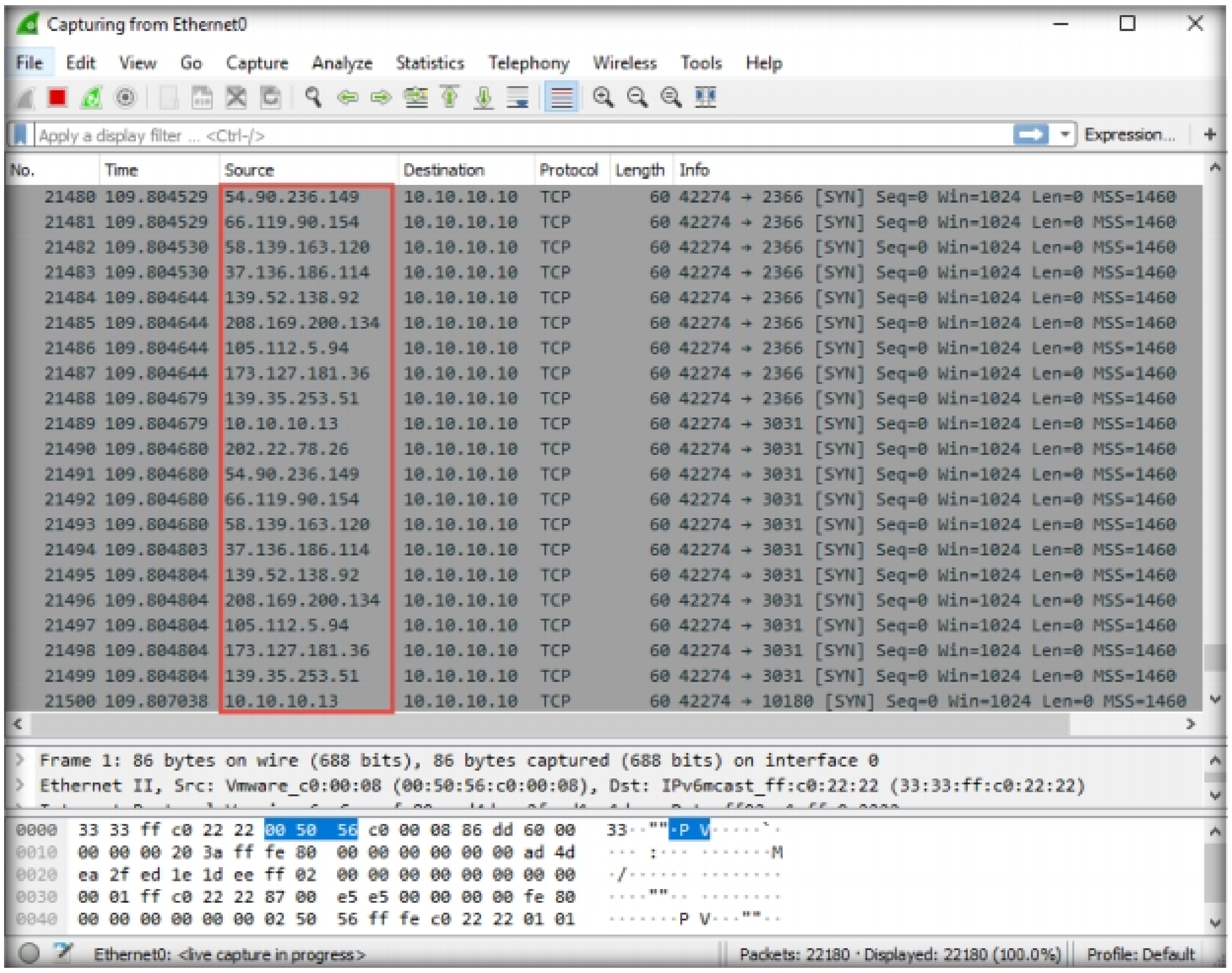


```
┌─[root@parrot]─[~]
└──╼ #nmap -D RND:10 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-25 08:36 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00082s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.62 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.1.7: Nmap Decoying IP Addresses

16. Now, return to the **Windows 10** virtual machine (target machine) and observe packets captured by Wireshark, which displays the multiple IP addresses in the source section, as shown in the screenshot.

Note: The results may vary in your lab environment.



```
No.   Time       Source          Destination  Protocol Length Info
21480 109.804529 54.90.236.149   10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21481 109.804529 66.119.90.154   10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21482 109.804530 58.139.163.120  10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21483 109.804530 37.136.186.114  10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21484 109.804644 139.52.138.92   10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21485 109.804644 208.169.200.134 10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21486 109.804644 105.112.5.94    10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21487 109.804644 173.127.181.36  10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21488 109.804679 139.35.253.51   10.10.10.10  TCP      60 42274 → 2366 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21489 109.804679 10.10.10.13     10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21490 109.804680 202.22.78.26    10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21491 109.804680 54.90.236.149   10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21492 109.804680 66.119.90.154   10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21493 109.804680 58.139.163.120  10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21494 109.804803 37.136.186.114  10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21495 109.804804 139.52.138.92   10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21496 109.804804 208.169.200.134 10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21497 109.804804 105.112.5.94    10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21498 109.804804 173.127.181.36  10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21499 109.804804 139.35.253.51   10.10.10.10  TCP      60 42274 → 3031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21500 109.807038 10.10.10.13     10.10.10.10  TCP      60 42274 → 10180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv6mcast_ff:c0:22:22 (33:33:ff:c0:22:22)
```

```
0000  33 33 ff c0 22 22 00 50  56 c0 00 08 86 dd 60 00   33··""·P V·····`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 ad 4d   ··· :··· ·······M
0020  ea 2f ed 1e 1d ee ff 02  00 00 00 00 00 00 00 00   ·/······ ········
0030  00 01 ff c0 22 22 87 00  e5 e5 00 00 00 00 fe 80   ····""·· ········
0040  00 00 00 00 00 00 02 50  56 ff fe c0 22 22 01 01   ·······P V···""··
```

Ethernet0: <live capture in progress> | Packets: 22180 · Displayed: 22180 (100.0%) | Profile: Default

Figure 4.1.8: Decoyed IP Addresses in Windows 10 Wireshark

17. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.

18. Close all open windows and document all the acquired information.

19. Turn off the **Parrot Security** virtual machine.

TASK 2

Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator**/**Pa$$w0rd**.

2. Install **Wireshark** available at **Z:\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** with all the default settings.

3. **Windows Server 2019** virtual machine will restart. Log in with the credentials **Administrator**/**Pa$$w0rd**.

4. Click on the **Start** menu and launch **Wireshark** from the applications.

5. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.

TASK 2.1

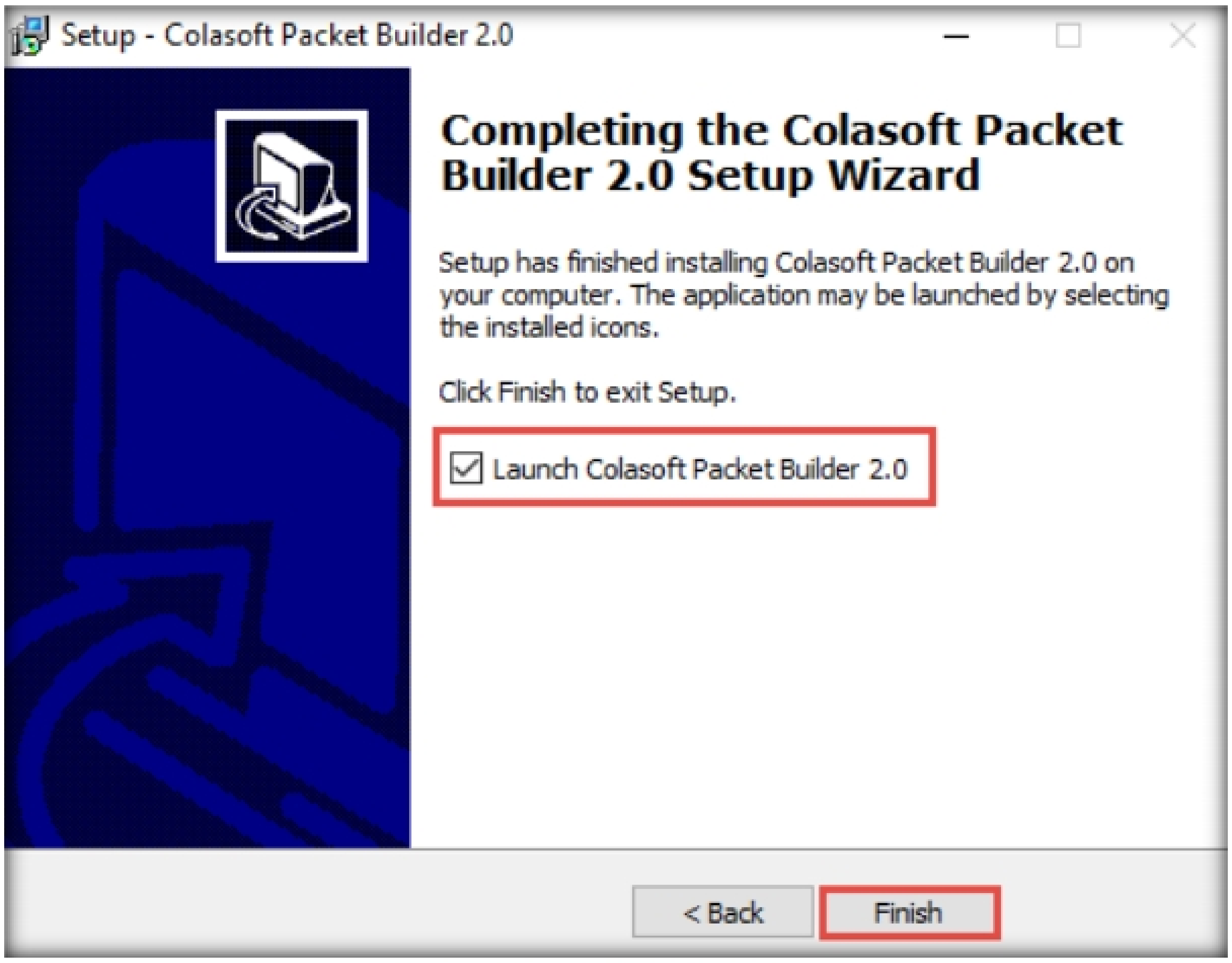
Install Colasoft Packet Builder

Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

6. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.212.exe**.

7. Follow the wizard-driven installation steps to install **Colasoft Packet Builder**.

8. After the completion of the installation, click on the **Launch Colasoft Packet Builder 2.0** checkbox and click **Finish**.



Completing the Colasoft Packet Builder 2.0 Setup Wizard

Setup has finished installing Colasoft Packet Builder 2.0 on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch Colasoft Packet Builder 2.0

Figure 4.2.1: Colasoft Packet Builder Setup

TASK 2.2

Choose a Network Interface

9. The **Colasoft Packet Builder** GUI appears; click on the **Adapter** icon, as shown in the screenshot.

Note: If a pop-up appears, close the window.

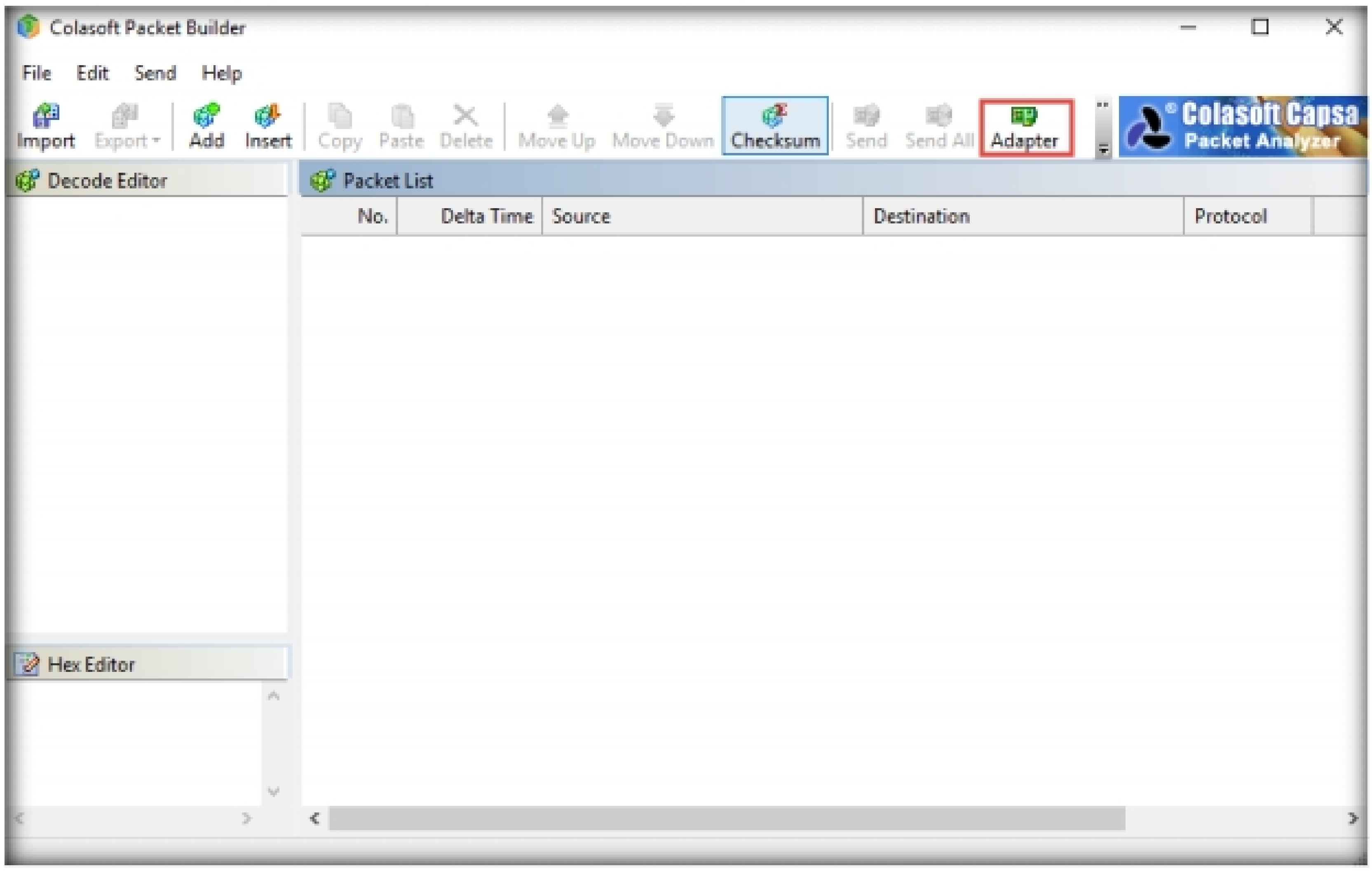
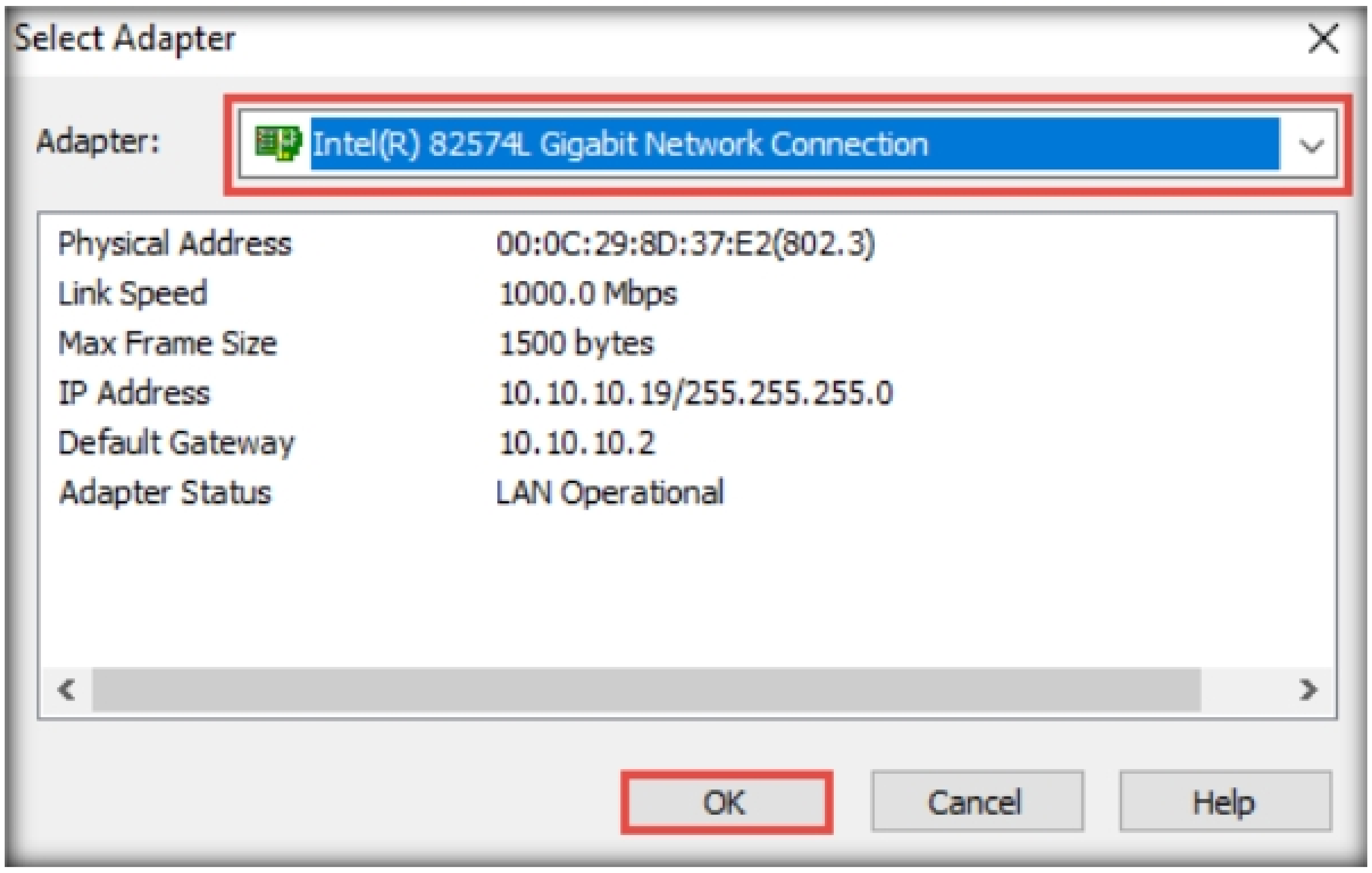

Colasoft Packet Builder
File
Edit
Send
Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Send All
Adapter
Colasoft Capsa
Packet Analyzer
Decode Editor
Packet List
No.
Delta Time
Source
Destination
Protocol
Hex Editor

Figure 4.2.2: Colasoft Packet Builder GUI: click on adapter icon

10. When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.

Note: The adapter configuration might differ in your lab environment.


Select Adapter
OK
Cancel
Help

Adapter: Intel(R) 82574L Gigabit Network Connection

Physical Address	00:0C:29:8D:37:E2(802.3)
Link Speed	1000.0 Mbps
Max Frame Size	1500 bytes
IP Address	10.10.10.19/255.255.255.0
Default Gateway	10.10.10.2
Adapter Status	LAN Operational

Figure 4.2.3: Choosing an adapter in Colasoft

TASK 2.3

Create an ARP Packet

11. To add or create a packet, click the **Add** (Add) icon in the **Menu** bar.

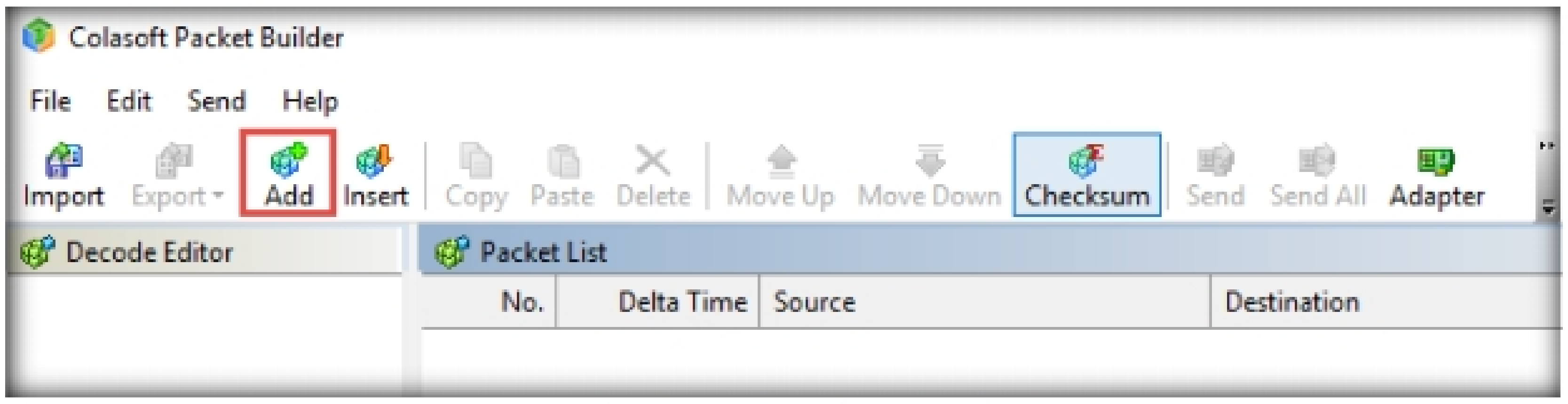
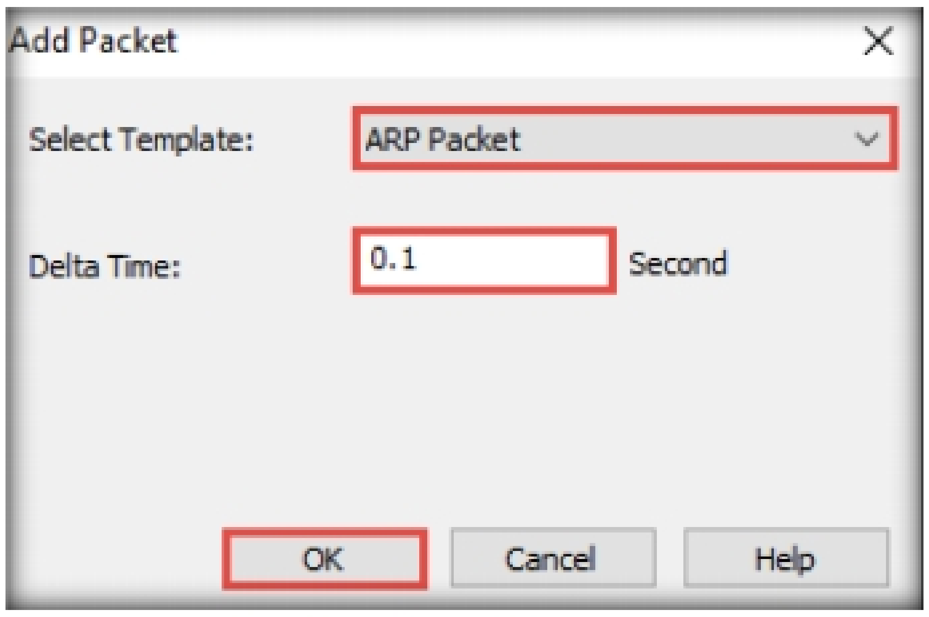

Colasoft Packet Builder
File
Edit
Send
Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Send All
Adapter
Decode Editor
Packet List
No.
Delta Time
Source
Destination

Figure 4.2.4: Adding a packet in Colasoft Packet Builder

12. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.

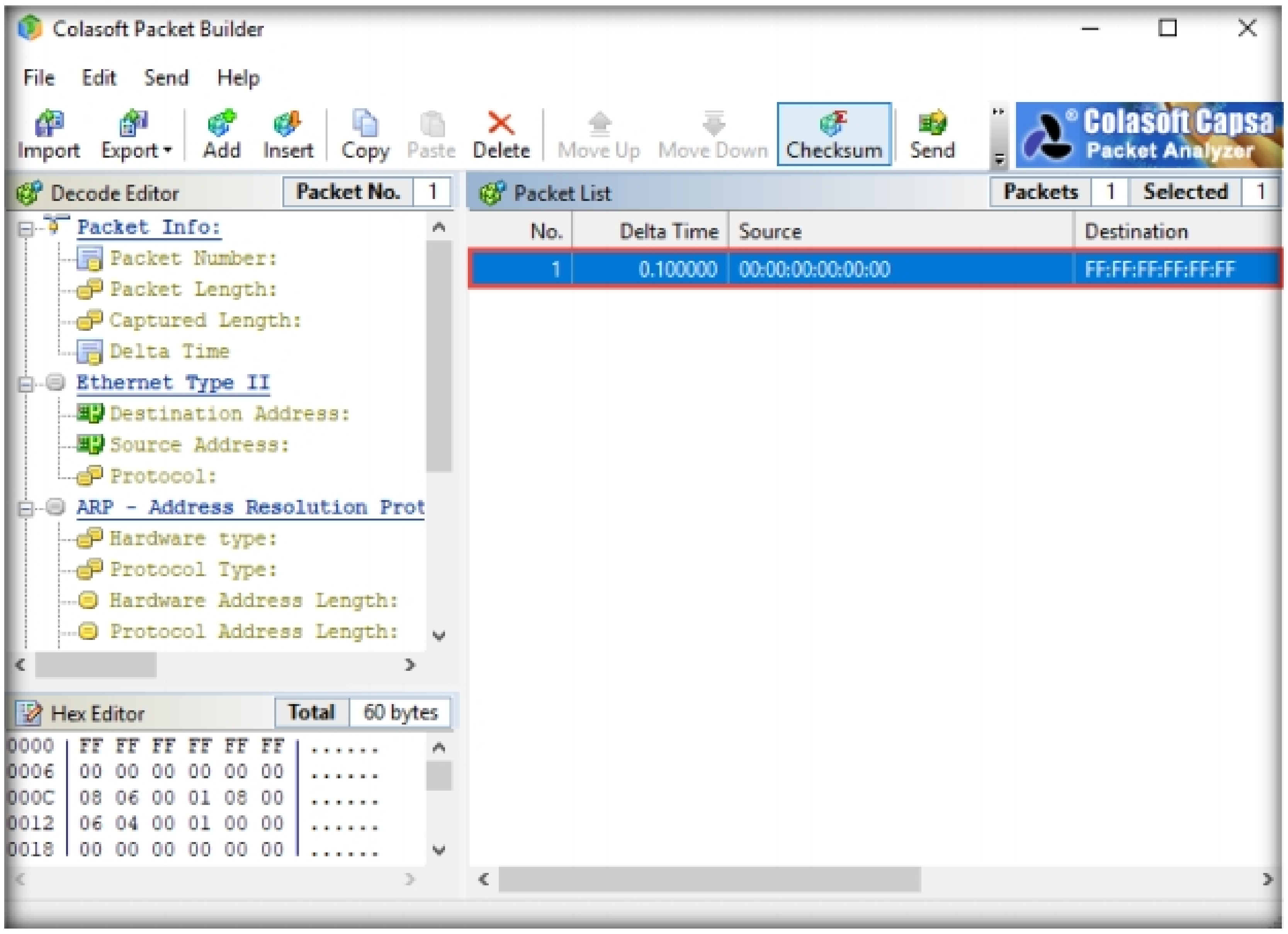

Add Packet
OK
Cancel
Help

Select Template: ARP Packet

Delta Time: 0.1 Second

Figure 4.2.5: Add Packet dialog box

13. You can view the added packets list on the right-hand side of the window, under **Packet List**.

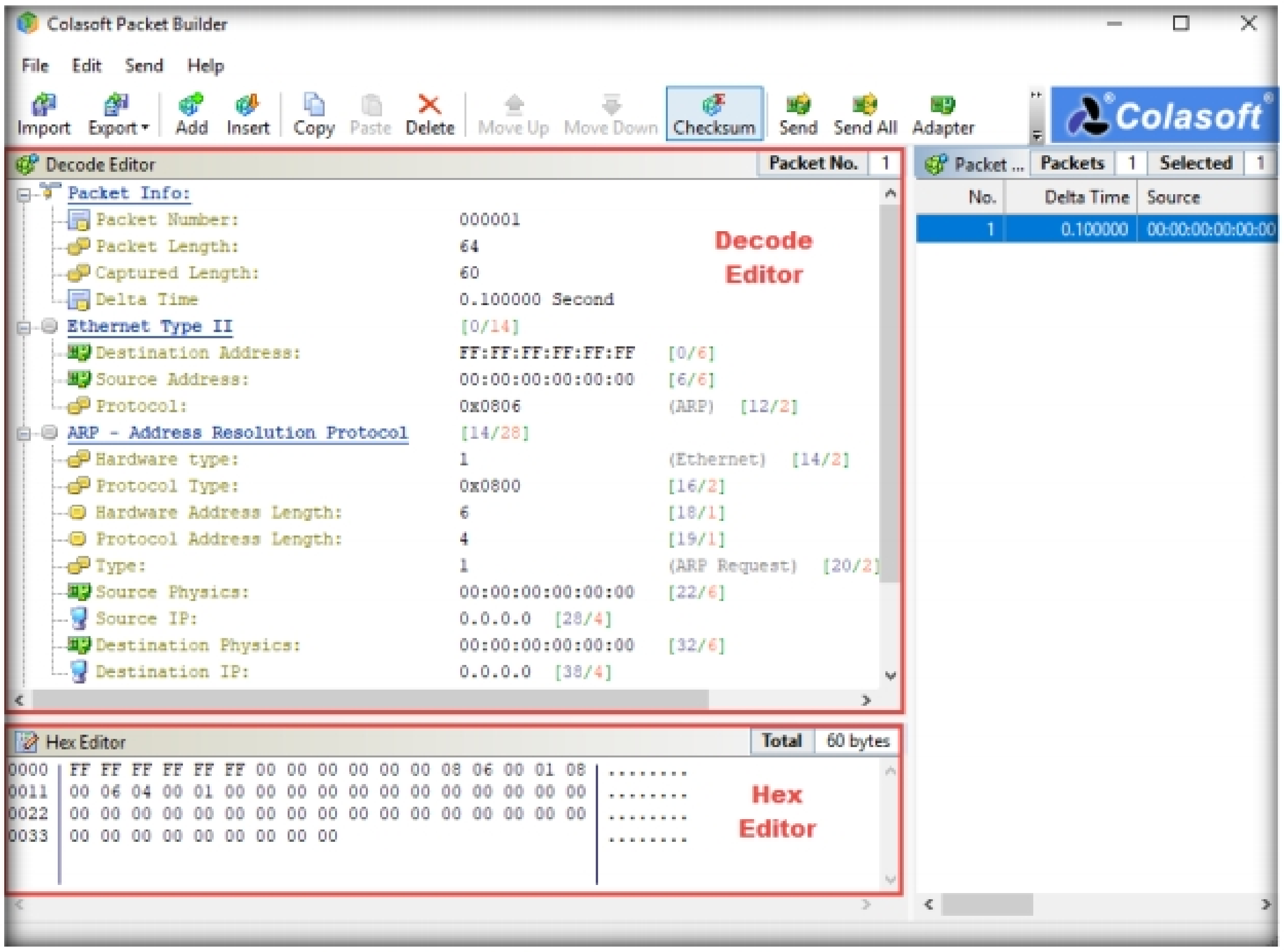

Colasoft Packet Builder
File
Edit
Send
Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Colasoft Capsa
Packet Analyzer
Decode Editor
Packet No. 1
Packet Info:
Packet Number:
Packet Length:
Captured Length:
Delta Time
Ethernet Type II
Destination Address:
Source Address:
Protocol:
ARP - Address Resolution Prot
Hardware type:
Protocol Type:
Hardware Address Length:
Protocol Address Length:
Packet List
Packets 1
Selected 1
Hex Editor
Total 60 bytes

No.	Delta Time	Source	Destination
1	0.100000	00:00:00:00:00:00	FF:FF:FF:FF:FF:FF

```
0000 | FF FF FF FF FF FF | ......
0006 | 00 00 00 00 00 00 | ......
000C | 08 06 00 01 08 00 | ......
0012 | 06 04 00 01 00 00 | ......
0018 | 00 00 00 00 00 00 | ......
```

Figure 4.2.6: Viewing the added packets

14. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.
    - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.
    - **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.


Colasoft Packet Builder
File
Edit
Send
Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Send All
Adapter
Colasoft
Decode Editor
Packet No. 1
Decode Editor
Hex Editor
Total 60 bytes
Hex Editor
Packet ...
Packets 1
Selected 1
No.
Delta Time
Source

```
Packet Info:
    Packet Number:                 000001
    Packet Length:                 64
    Captured Length:               60
    Delta Time                     0.100000 Second
Ethernet Type II                   [0/14]
    Destination Address:           FF:FF:FF:FF:FF:FF    [0/6]
    Source Address:                00:00:00:00:00:00    [6/6]
    Protocol:                      0x0806               (ARP)   [12/2]
ARP - Address Resolution Protocol  [14/28]
    Hardware type:                 1                    (Ethernet)   [14/2]
    Protocol Type:                 0x0800               [16/2]
    Hardware Address Length:       6                    [18/1]
    Protocol Address Length:       4                    [19/1]
    Type:                          1                    (ARP Request)   [20/2]
    Source Physics:                00:00:00:00:00:00    [22/6]
    Source IP:                     0.0.0.0   [28/4]
    Destination Physics:           00:00:00:00:00:00    [32/6]
    Destination IP:                0.0.0.0   [38/4]
```

```
0000 | FF FF FF FF FF FF 00 00 00 00 00 00 08 06 00 01 08 | ........
0011 | 00 06 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 | ........
0022 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........
0033 | 00 00 00 00 00 00 00 00 00                         | ........
```

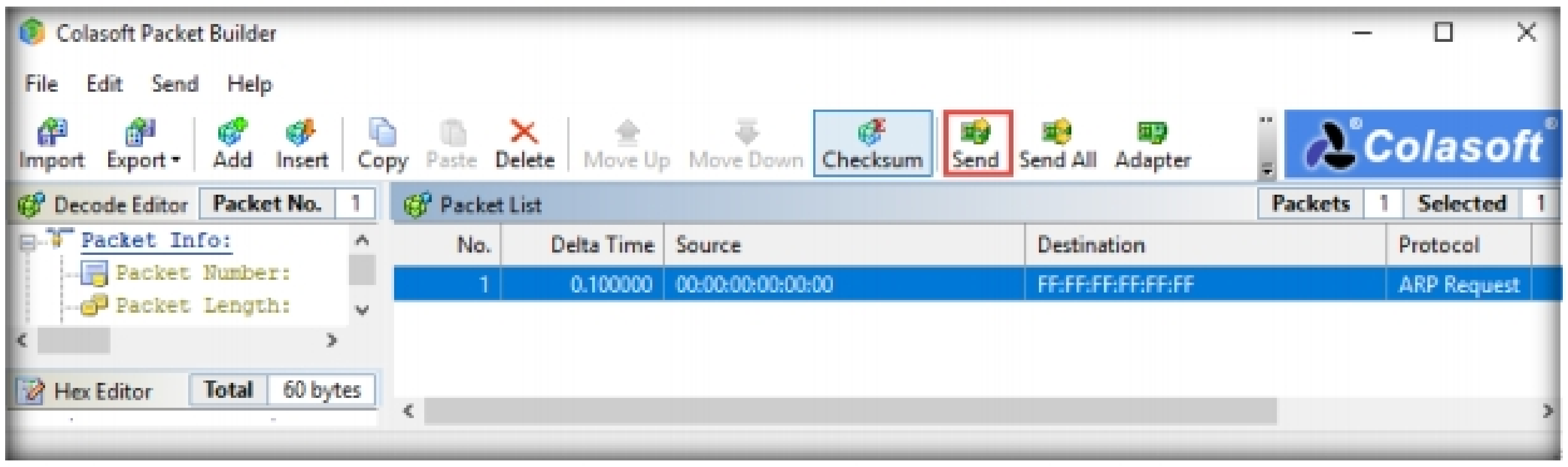
No.	Delta Time	Source
1	0.100000	00:00:00:00:00:00

Figure 4.2.7: Colasoft Packet Builder Decode and Hex Editors

TASK 2.4

Send the Created ARP Packet to the Target

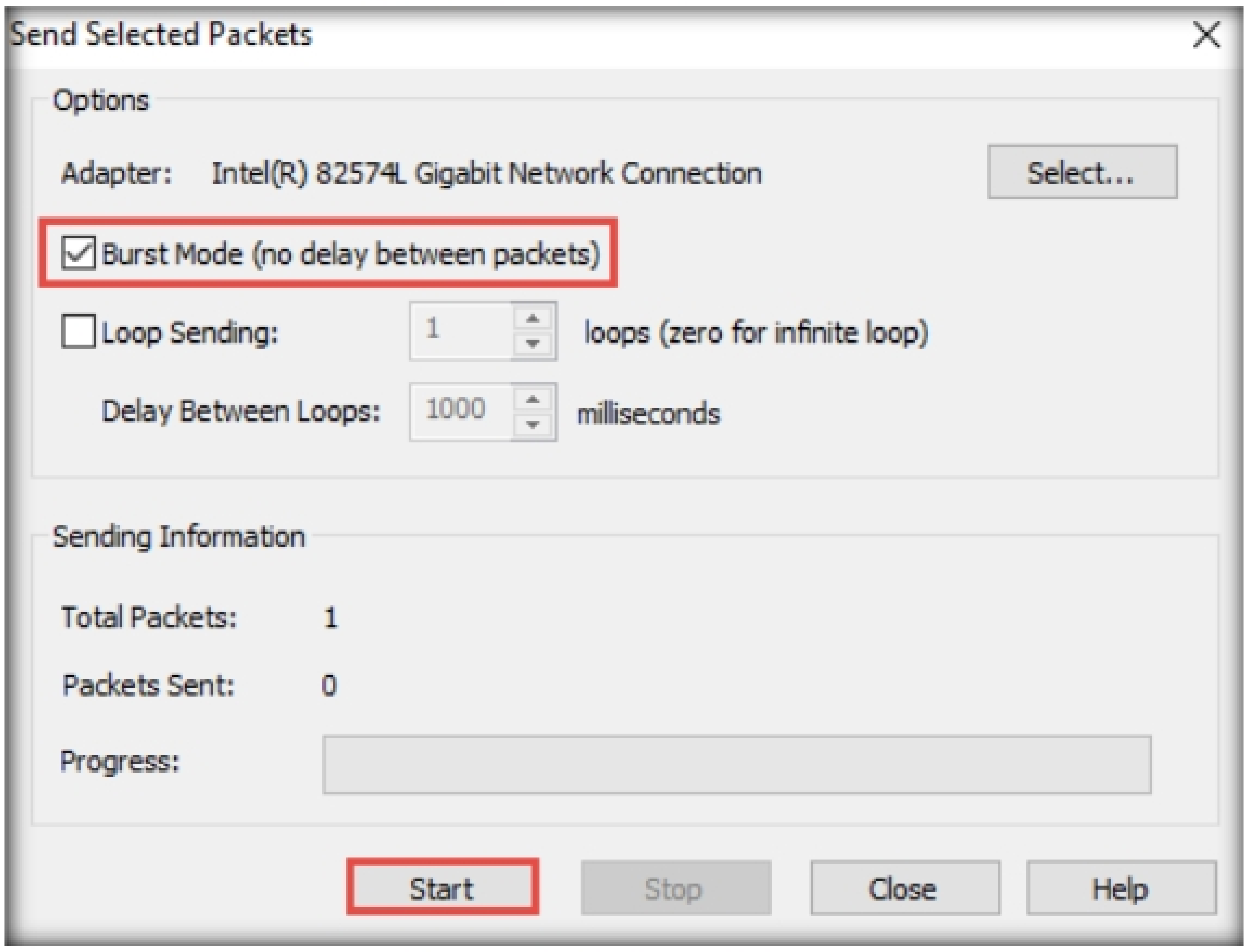
15. To send the packet, click **Send** from the **Menu** bar.


Colasoft Packet Builder
File
Edit
Send
Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Send All
Adapter
Colasoft
Decode Editor
Packet No. 1
Packet Info:
Packet Number:
Packet Length:
Hex Editor
Total 60 bytes
Packet List
Packets 1
Selected 1

No.	Delta Time	Source	Destination	Protocol
1	0.100000	00:00:00:00:00:00	FF:FF:FF:FF:FF:FF	ARP Request

Figure 4.2.8: Sending all packets

16. In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.


Send Selected Packets

Options

Adapter: Intel(R) 82574L Gigabit Network Connection

☑ Burst Mode (no delay between packets)

☐ Loop Sending: 1 loops (zero for infinite loop)

Delay Between Loops: 1000 milliseconds

Sending Information

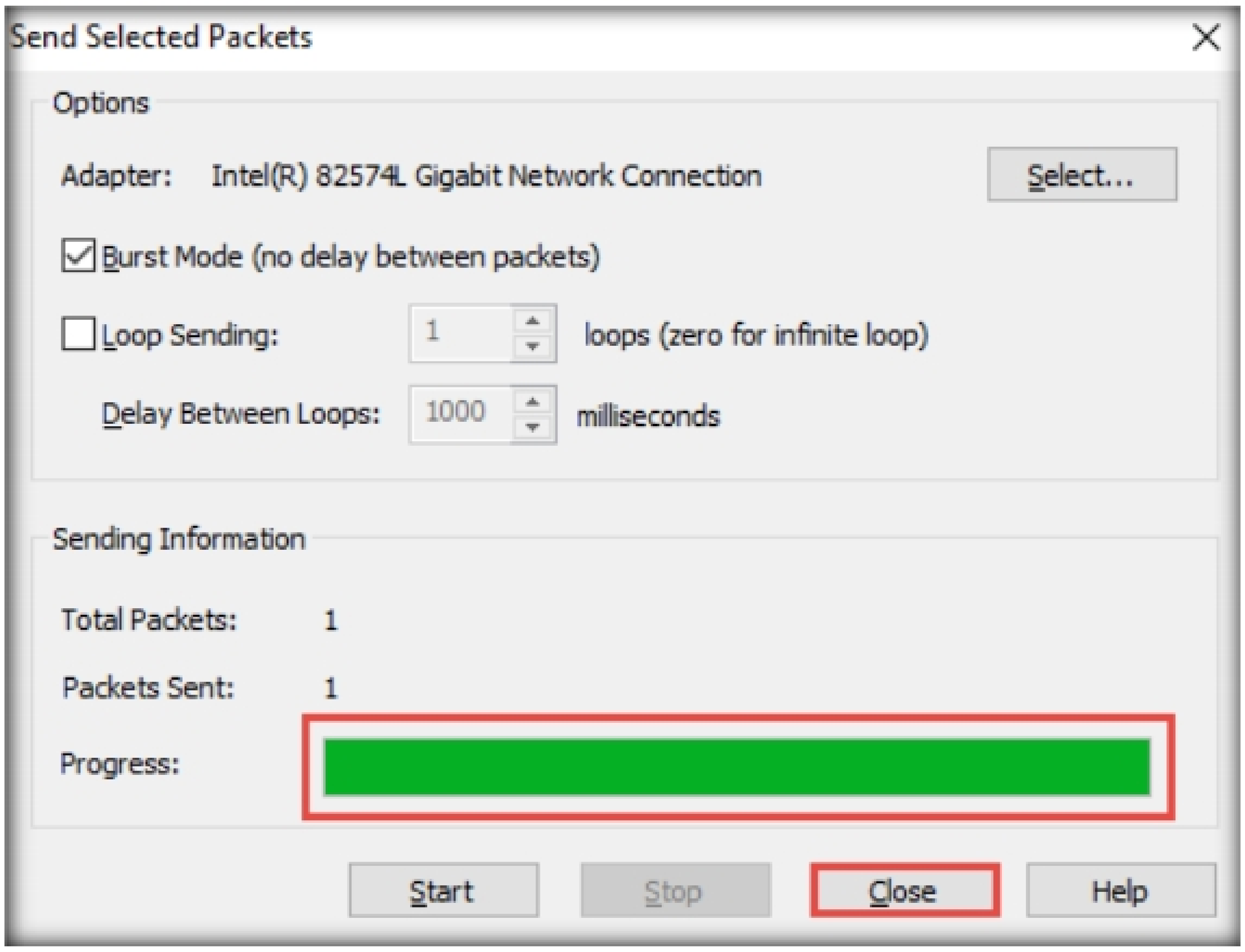
Total Packets: 1

Packets Sent: 0

Progress:

Figure 4.2.9: Setting Burst Mode option

17. After the **Progress** bar completes, click **Close**.


Send Selected Packets

Options

Adapter: Intel(R) 82574L Gigabit Network Connection

☑ Burst Mode (no delay between packets)

☐ Loop Sending: 1 loops (zero for infinite loop)

Delay Between Loops: 1000 milliseconds

Sending Information

Total Packets: 1

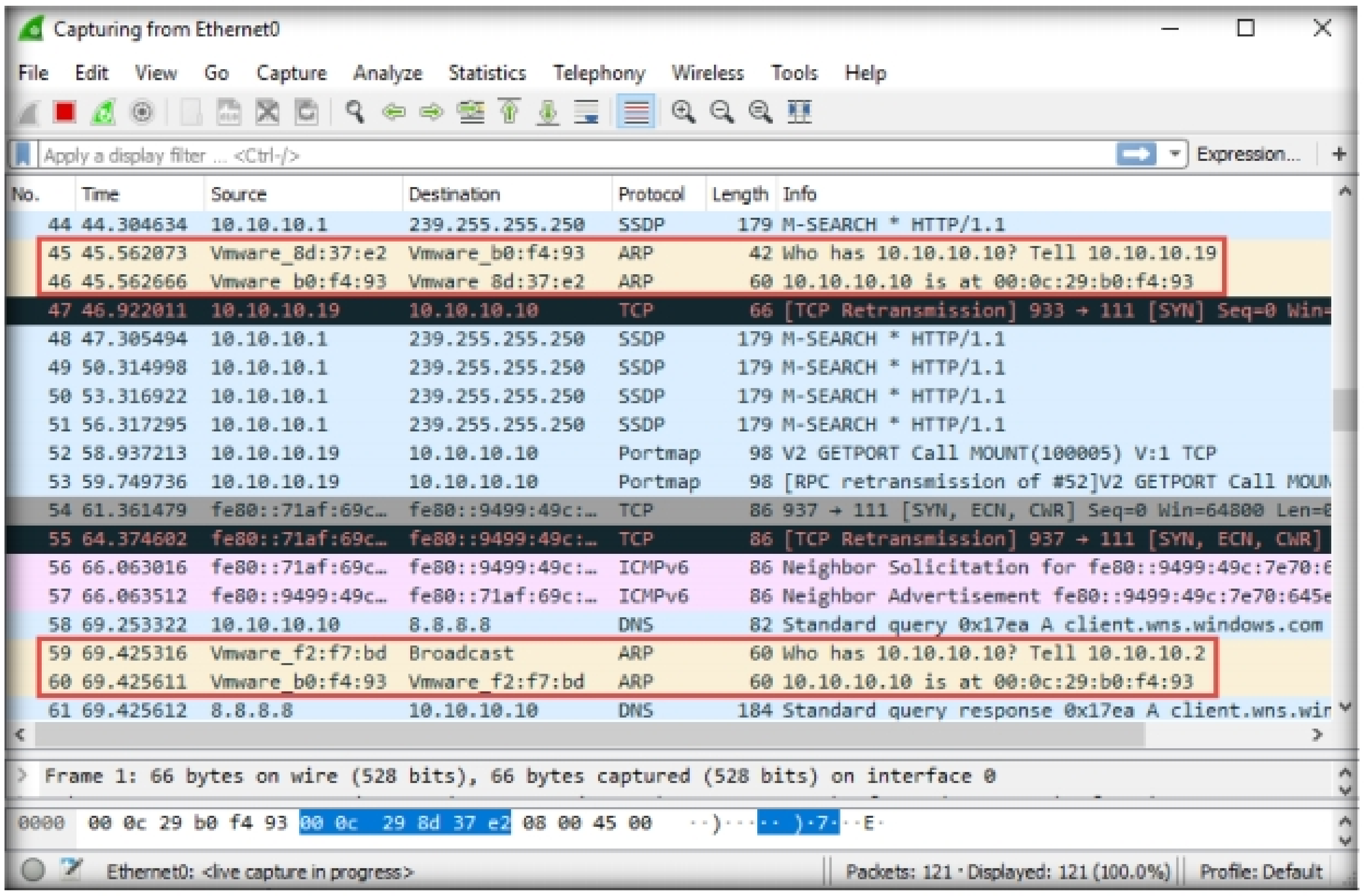
Packets Sent: 1

Progress:

Figure 4.2.10: All packets successfully sent

18. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

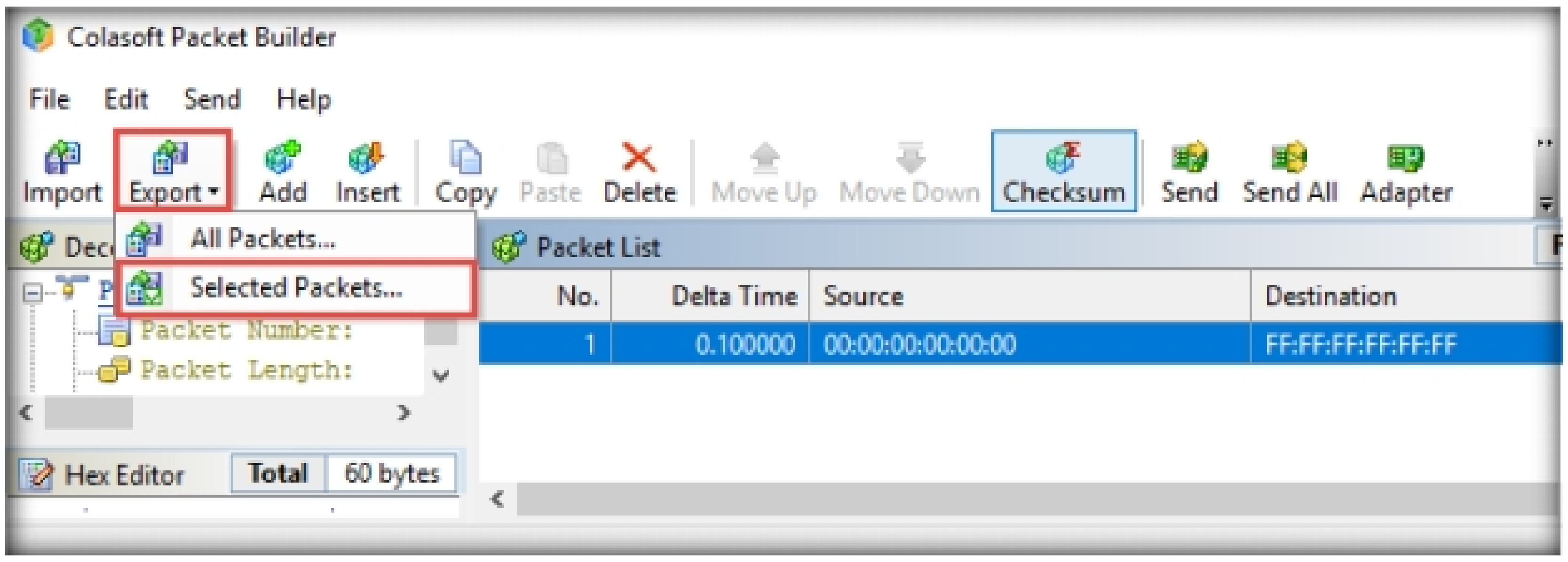
Note: Here, the host machine (**10.10.10.19**) is broadcasting ARP packets, prompting the target machine (**10.10.10.10**) to reply to the message.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Ethernet0: <live capture in progress>
Packets: 121 · Displayed: 121 (100.0%)
Profile: Default

```
No.  Time       Source              Destination         Protocol  Length Info
  44 44.304634  10.10.10.1          239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
  45 45.562073  Vmware_8d:37:e2     Vmware_b0:f4:93     ARP        42 Who has 10.10.10.10? Tell 10.10.10.19
  46 45.562666  Vmware_b0:f4:93     Vmware_8d:37:e2     ARP        60 10.10.10.10 is at 00:0c:29:b0:f4:93
  47 46.922011  10.10.10.19         10.10.10.10         TCP        66 [TCP Retransmission] 933 → 111 [SYN] Seq=0 Win=
  48 47.305494  10.10.10.1          239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
  49 50.314998  10.10.10.1          239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
  50 53.316922  10.10.10.1          239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
  51 56.317295  10.10.10.1          239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
  52 58.937213  10.10.10.19         10.10.10.10         Portmap    98 V2 GETPORT Call MOUNT(100005) V:1 TCP
  53 59.749736  10.10.10.19         10.10.10.10         Portmap    98 [RPC retransmission of #52]V2 GETPORT Call MOUN
  54 61.361479  fe80::71af:69c…     fe80::9499:49c:…    TCP        86 937 → 111 [SYN, ECN, CWR] Seq=0 Win=64800 Len=
  55 64.374602  fe80::71af:69c…     fe80::9499:49c:…    TCP        86 [TCP Retransmission] 937 → 111 [SYN, ECN, CWR]
  56 66.063016  fe80::71af:69c…     fe80::9499:49c:…    ICMPv6     86 Neighbor Solicitation for fe80::9499:49c:7e70:
  57 66.063512  fe80::9499:49c…     fe80::71af:69c:…    ICMPv6     86 Neighbor Advertisement fe80::9499:49c:7e70:645
  58 69.253322  10.10.10.10         8.8.8.8             DNS        82 Standard query 0x17ea A client.wns.windows.com
  59 69.425316  Vmware_f2:f7:bd     Broadcast           ARP        60 Who has 10.10.10.10? Tell 10.10.10.2
  60 69.425611  Vmware_b0:f4:93     Vmware_f2:f7:bd     ARP        60 10.10.10.10 is at 00:0c:29:b0:f4:93
  61 69.425612  8.8.8.8             10.10.10.10         DNS       184 Standard query response 0x17ea A client.wns.wir

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

0000  00 0c 29 b0 f4 93 00 0c  29 8d 37 e2 08 00 45 00   ··)·····)·7···E·
```

Figure 4.2.11: Wireshark captured packets

19. To export the packet, click **Export → Selected Packets...**.


Colasoft Packet Builder
File Edit Send Help
Import
Export
Add
Insert
Copy
Paste
Delete
Move Up
Move Down
Checksum
Send
Send All
Adapter
All Packets...
Selected Packets...
Packet Number:
Packet Length:
Hex Editor
Total 60 bytes
Packet List

No.	Delta Time	Source	Destination
1	0.100000	00:00:00:00:00:00	FF:FF:FF:FF:FF:FF

Figure 4.2.12: Exporting the packets in Colasoft

20. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.

21. This saved file can be used for future reference.

22. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.

23. Close all open windows and document all the acquired information.

24. Turn off the **Windows Server 2019** virtual machine.

TASK 3

Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

Note: Before beginning this task, ensure that the **Windows 10** virtual machine is running and that **Windows Defender Firewall** is enabled.

1. In the **Windows 10** virtual machine, launch **Wireshark** and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
2. Turn on the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

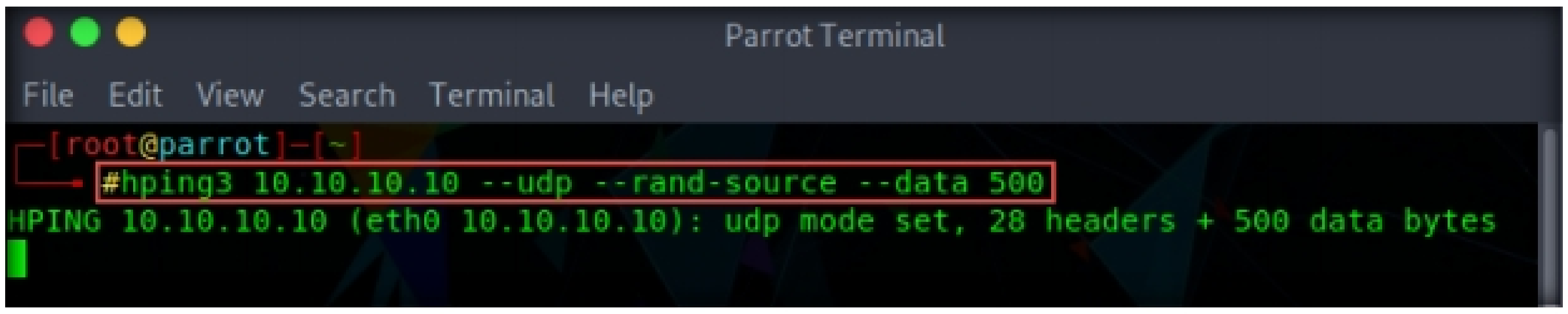
7. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Perform UDP Packet Crafting

8. In the terminal window, type **hping3 <Target IP Address> --udp --rand-source --data 500** (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

Note: Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size.



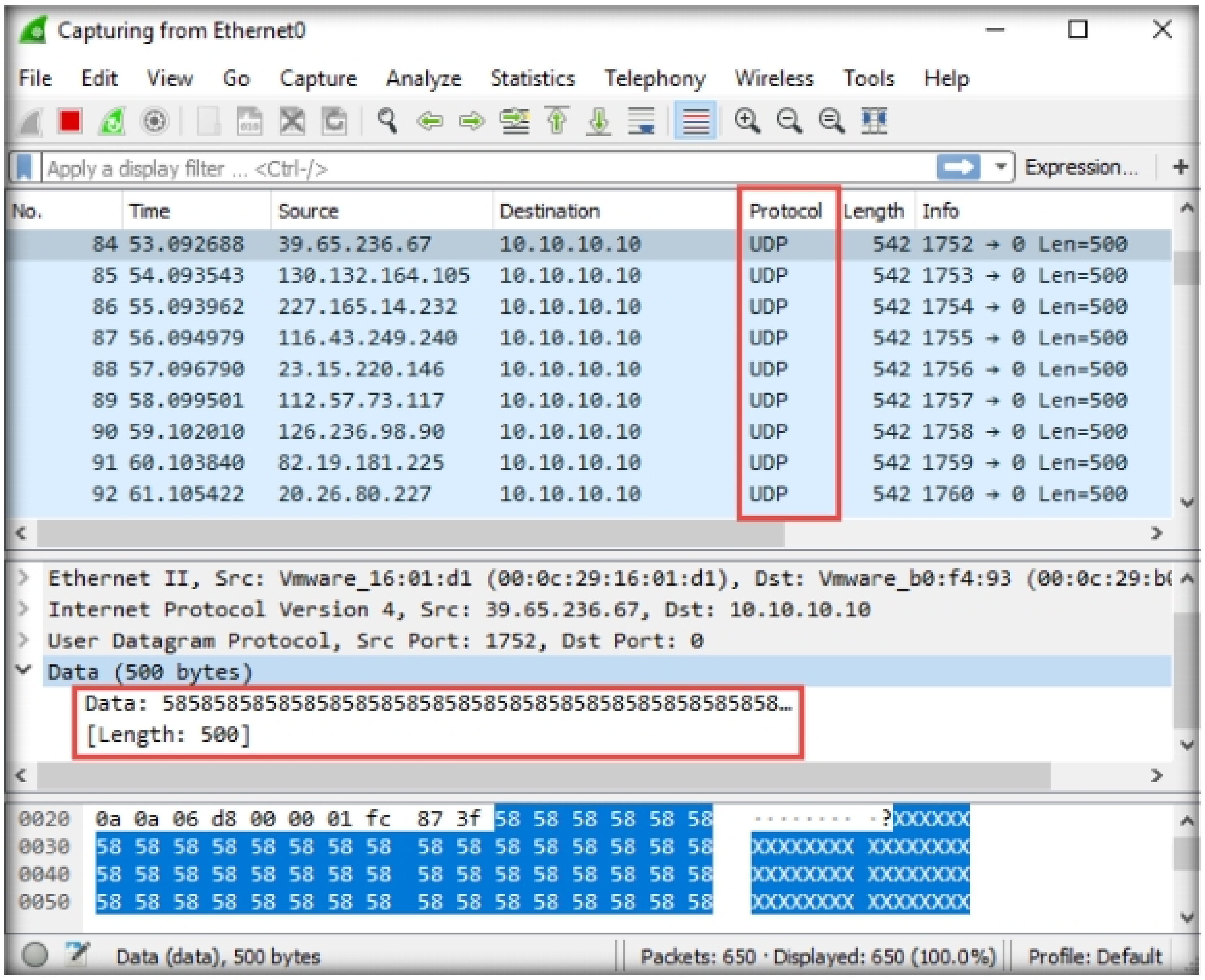
```
┌─[root@parrot]─[~]
└──╼ #hping3 10.10.10.10 --udp --rand-source --data 500
HPING 10.10.10.10 (eth0 10.10.10.10): udp mode set, 28 headers + 500 data bytes
```

Figure 4.3.1: Hping3 Output of 3 Packets sent to the target machine

9. Now, switch to the **Windows 10** virtual machine and observe the UDP packets captured by **Wireshark**.

Note: You can double-click any UDP packet and observe the details.

10. Expand the **Data** node in the **Packet Details** pane and observe the size of **Data** and its **Length** (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., **500**).


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
84	53.092688	39.65.236.67	10.10.10.10	UDP	542	1752 → 0 Len=500
85	54.093543	130.132.164.105	10.10.10.10	UDP	542	1753 → 0 Len=500
86	55.093962	227.165.14.232	10.10.10.10	UDP	542	1754 → 0 Len=500
87	56.094979	116.43.249.240	10.10.10.10	UDP	542	1755 → 0 Len=500
88	57.096790	23.15.220.146	10.10.10.10	UDP	542	1756 → 0 Len=500
89	58.099501	112.57.73.117	10.10.10.10	UDP	542	1757 → 0 Len=500
90	59.102010	126.236.98.90	10.10.10.10	UDP	542	1758 → 0 Len=500
91	60.103840	82.19.181.225	10.10.10.10	UDP	542	1759 → 0 Len=500
92	61.105422	20.26.80.227	10.10.10.10	UDP	542	1760 → 0 Len=500

```
> Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_b0:f4:93 (00:0c:29:b
> Internet Protocol Version 4, Src: 39.65.236.67, Dst: 10.10.10.10
> User Datagram Protocol, Src Port: 1752, Dst Port: 0
v Data (500 bytes)
    Data: 5858585858585858585858585858585858585858585858585858…
    [Length: 500]
```

```
0020  0a 0a 06 d8 00 00 01 fc  87 3f 58 58 58 58 58 58   ·········?XXXXXX
0030  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
```

```
Data (data), 500 bytes | Packets: 650 · Displayed: 650 (100.0%) | Profile: Default
```

Figure 4.3.2: Wireshark capturing UDP packets in the target machine (Windows 10)

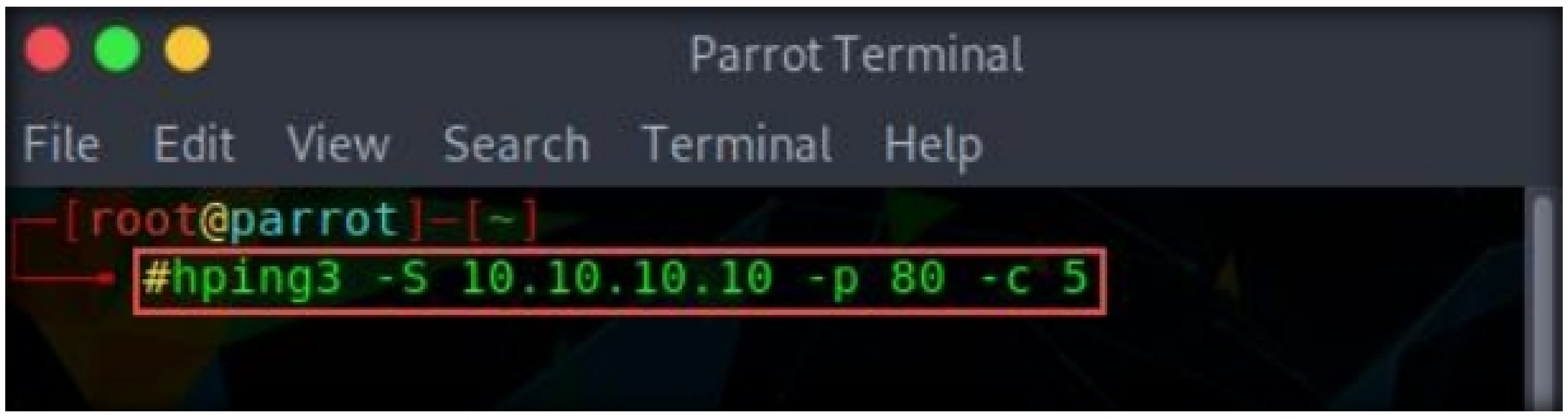
TASK 3.2

Send TCP SYN Request

11. Switch to the **Parrot Security** virtual machine. In the **Parrot Terminal** window, first press **Control+C** and type **hping3 -S <Target IP Address> -p 80 -c 5** (here, target IP address is **10.10.10.10**), and then press **Enter**.

Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

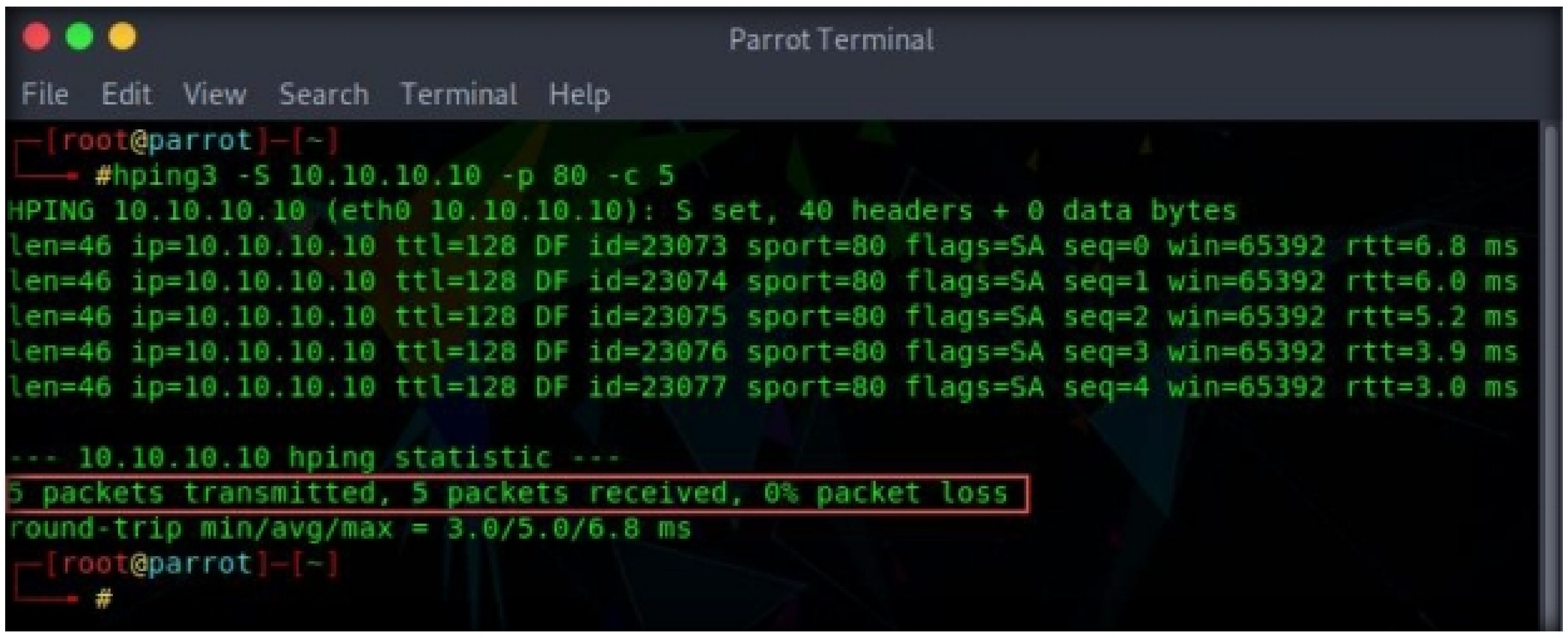
Note: The IP addresses might vary in your lab environment.



```
[root@parrot]-[~]
#hping3 -S 10.10.10.10 -p 80 -c 5
```

Figure 4.3.3: Hping3 sending TCP SYN packets

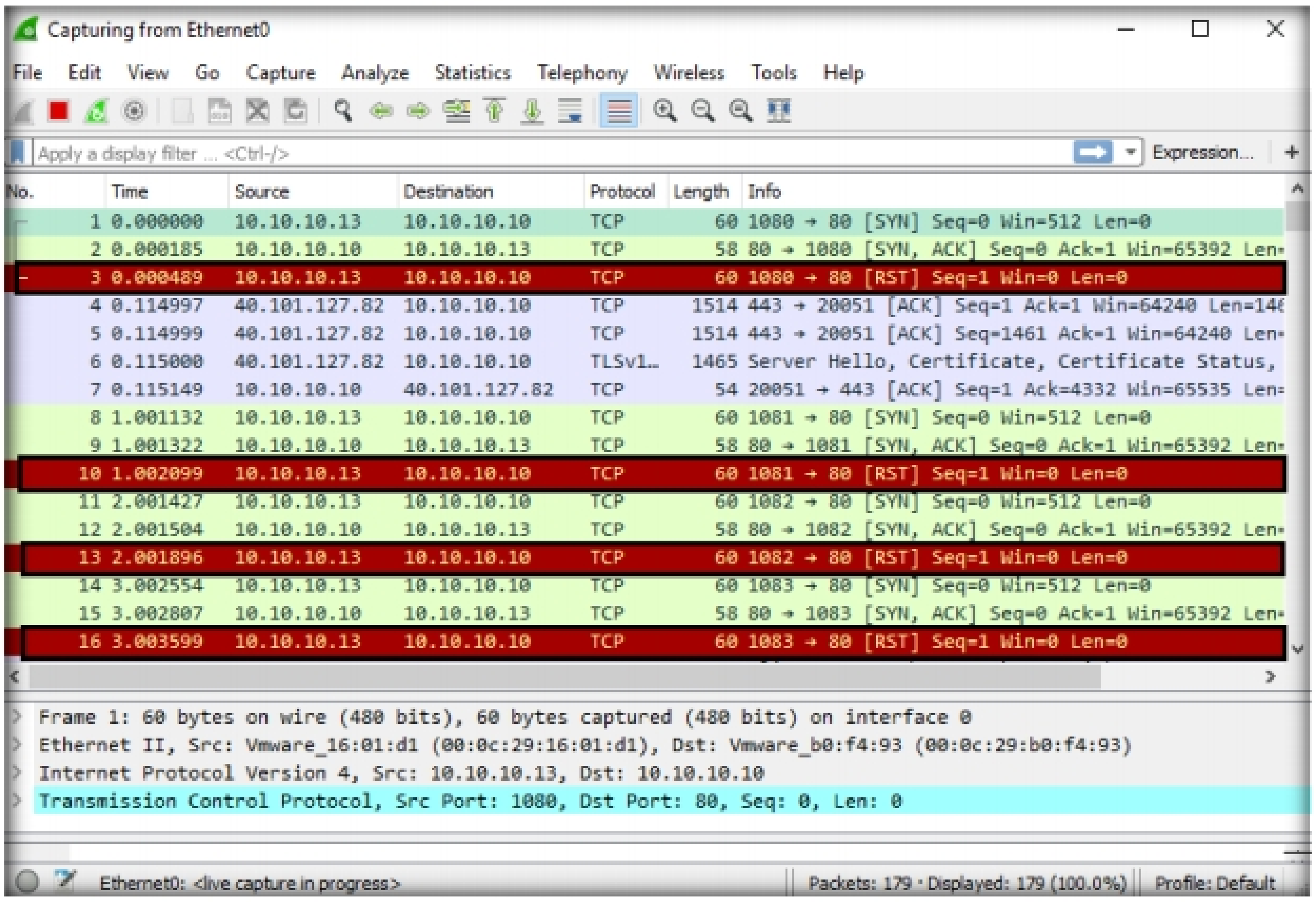
12. In the result, it is indicated that five packets were sent and received through port 80.



```
┌─[root@parrot]─[~]
└──╼ #hping3 -S 10.10.10.10 -p 80 -c 5
HPING 10.10.10.10 (eth0 10.10.10.10): S set, 40 headers + 0 data bytes
len=46 ip=10.10.10.10 ttl=128 DF id=23073 sport=80 flags=SA seq=0 win=65392 rtt=6.8 ms
len=46 ip=10.10.10.10 ttl=128 DF id=23074 sport=80 flags=SA seq=1 win=65392 rtt=6.0 ms
len=46 ip=10.10.10.10 ttl=128 DF id=23075 sport=80 flags=SA seq=2 win=65392 rtt=5.2 ms
len=46 ip=10.10.10.10 ttl=128 DF id=23076 sport=80 flags=SA seq=3 win=65392 rtt=3.9 ms
len=46 ip=10.10.10.10 ttl=128 DF id=23077 sport=80 flags=SA seq=4 win=65392 rtt=3.0 ms

--- 10.10.10.10 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.0/5.0/6.8 ms
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.3.4: Hping3 sent TCP SYN packets to the target machine

13. Now, switch to the target machine (i.e., **Windows 10**) and observe the TCP packets captured via Wireshark.


Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source          Destination     Protocol  Length Info
    1 0.000000  10.10.10.13     10.10.10.10     TCP         60 1080 → 80 [SYN] Seq=0 Win=512 Len=0
    2 0.000185  10.10.10.10     10.10.10.13     TCP         58 80 → 1080 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=
    3 0.000489  10.10.10.13     10.10.10.10     TCP         60 1080 → 80 [RST] Seq=1 Win=0 Len=0
    4 0.114997  40.101.127.82   10.10.10.10     TCP       1514 443 → 20051 [ACK] Seq=1 Ack=1 Win=64240 Len=14
    5 0.114999  40.101.127.82   10.10.10.10     TCP       1514 443 → 20051 [ACK] Seq=1461 Ack=1 Win=64240 Len=
    6 0.115000  40.101.127.82   10.10.10.10     TLSv1…    1465 Server Hello, Certificate, Certificate Status,
    7 0.115149  10.10.10.10     40.101.127.82   TCP         54 20051 → 443 [ACK] Seq=1 Ack=4332 Win=65535 Len=
    8 1.001132  10.10.10.13     10.10.10.10     TCP         60 1081 → 80 [SYN] Seq=0 Win=512 Len=0
    9 1.001322  10.10.10.10     10.10.10.13     TCP         58 80 → 1081 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=
   10 1.002099  10.10.10.13     10.10.10.10     TCP         60 1081 → 80 [RST] Seq=1 Win=0 Len=0
   11 2.001427  10.10.10.13     10.10.10.10     TCP         60 1082 → 80 [SYN] Seq=0 Win=512 Len=0
   12 2.001504  10.10.10.10     10.10.10.13     TCP         58 80 → 1082 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=
   13 2.001896  10.10.10.13     10.10.10.10     TCP         60 1082 → 80 [RST] Seq=1 Win=0 Len=0
   14 3.002554  10.10.10.13     10.10.10.10     TCP         60 1083 → 80 [SYN] Seq=0 Win=512 Len=0
   15 3.002807  10.10.10.10     10.10.10.13     TCP         58 80 → 1083 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=
   16 3.003599  10.10.10.13     10.10.10.10     TCP         60 1083 → 80 [RST] Seq=1 Win=0 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)
> Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
> Transmission Control Protocol, Src Port: 1080, Dst Port: 80, Seq: 0, Len: 0
```

Ethernet0: <live capture in progress>
Packets: 179 · Displayed: 179 (100.0%)
Profile: Default

Figure 4.3.5: Wireshark TCP SYN Packets captured in the target machine

TASK 3.3

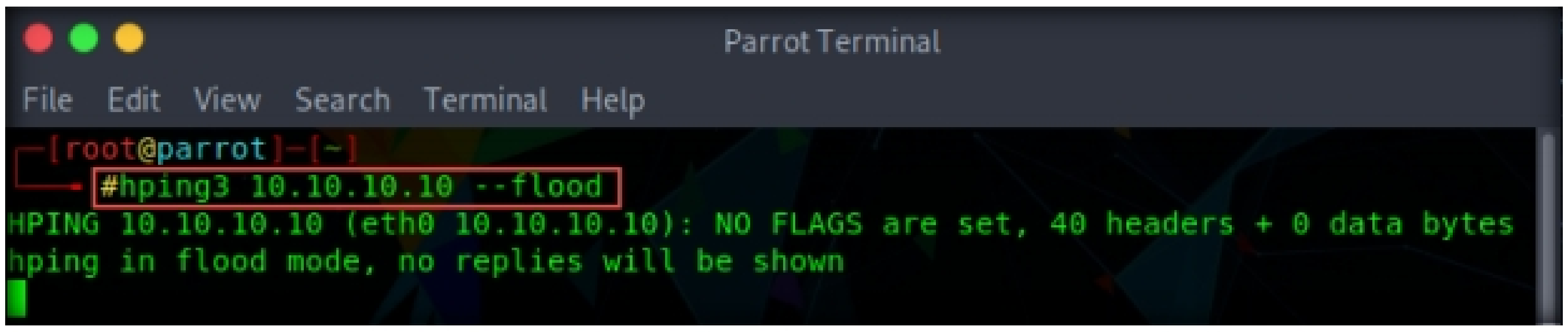
Perform TCP Flooding

14. Switch to the **Parrot Security** virtual machine and try to flood the target machine (here, **Windows 10**) with TCP packets.

15. In the **Parrot Terminal** window, type **hping3 <Target IP Address> --flood** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: **--flood**: performs the TCP flooding.

16. Once you flood traffic to the target machine, it will respond in the **hping3** terminal.



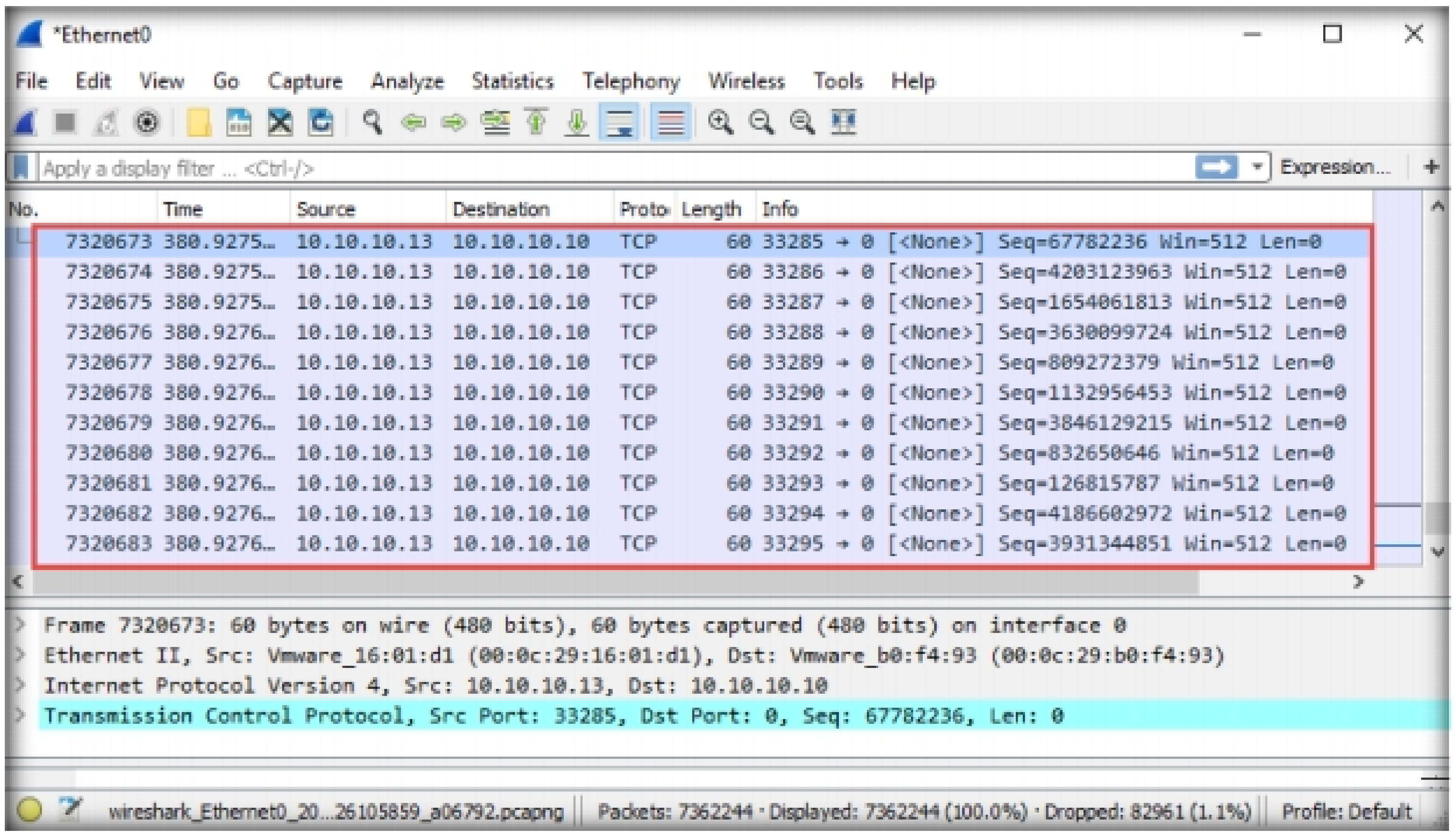
```
┌─[root@parrot]─[~]
└──╼ #hping3 10.10.10.10 --flood
HPING 10.10.10.10 (eth0 10.10.10.10): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 4.3.6: TCP Packets flooded to Target machine

17. Switch to **Windows 10** (target machine) and stop the packet capture in the Wireshark window after a while.

18. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine.

Note: You can double-click the TCP packet stream to observe the TCP packet information.


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

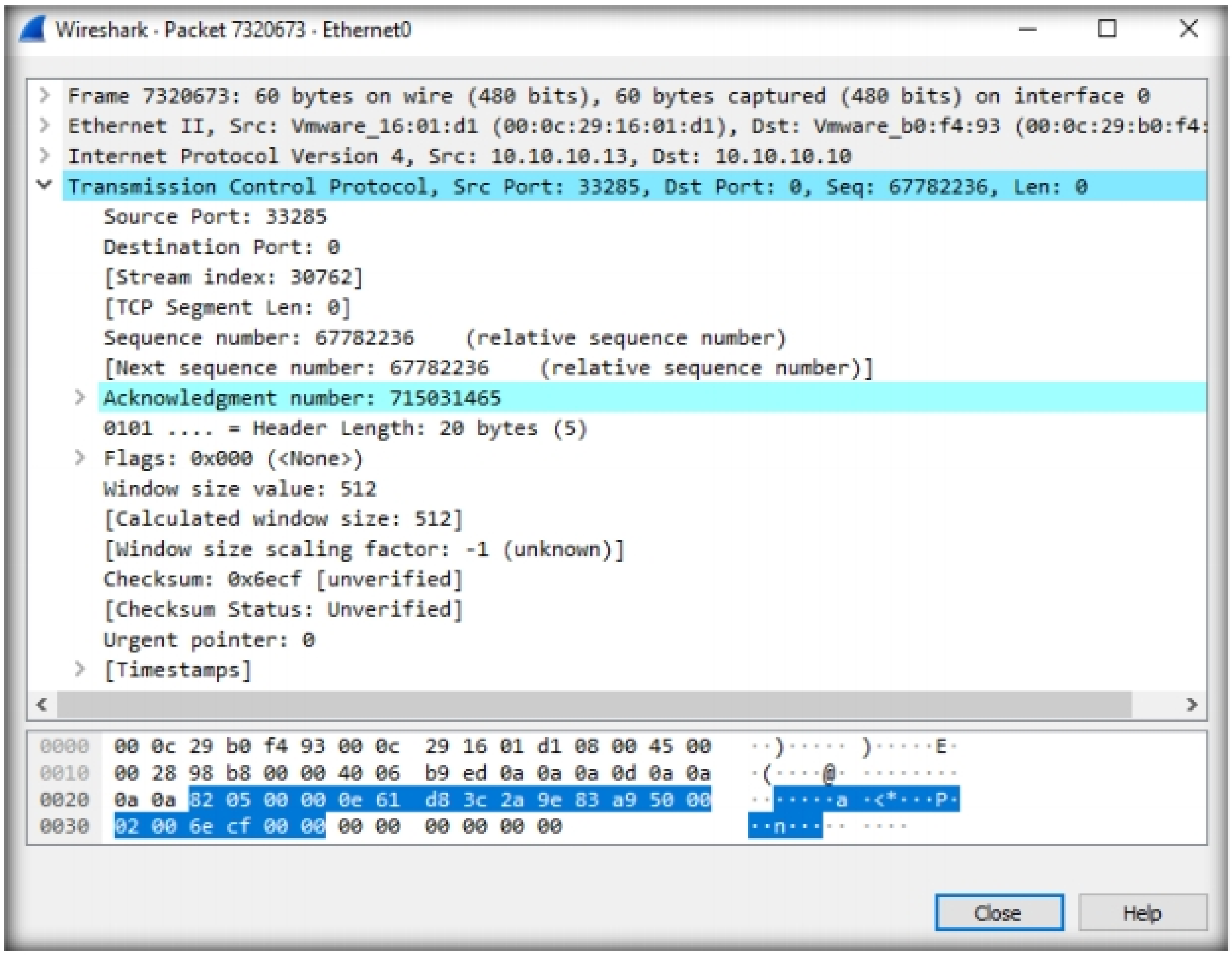
No.	Time	Source	Destination	Proto	Length	Info
7320673	380.9275…	10.10.10.13	10.10.10.10	TCP	60	33285 → 0 [<None>] Seq=67782236 Win=512 Len=0
7320674	380.9275…	10.10.10.13	10.10.10.10	TCP	60	33286 → 0 [<None>] Seq=4203123963 Win=512 Len=0
7320675	380.9275…	10.10.10.13	10.10.10.10	TCP	60	33287 → 0 [<None>] Seq=1654061813 Win=512 Len=0
7320676	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33288 → 0 [<None>] Seq=3630099724 Win=512 Len=0
7320677	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33289 → 0 [<None>] Seq=809272379 Win=512 Len=0
7320678	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33290 → 0 [<None>] Seq=1132956453 Win=512 Len=0
7320679	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33291 → 0 [<None>] Seq=3846129215 Win=512 Len=0
7320680	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33292 → 0 [<None>] Seq=832650646 Win=512 Len=0
7320681	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33293 → 0 [<None>] Seq=126815787 Win=512 Len=0
7320682	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33294 → 0 [<None>] Seq=4186602972 Win=512 Len=0
7320683	380.9276…	10.10.10.13	10.10.10.10	TCP	60	33295 → 0 [<None>] Seq=3931344851 Win=512 Len=0

```
> Frame 7320673: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:93)
> Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
> Transmission Control Protocol, Src Port: 33285, Dst Port: 0, Seq: 67782236, Len: 0
```

wireshark_Ethernet0_20...26105859_a06792.pcapng | Packets: 7362244 · Displayed: 7362244 (100.0%) · Dropped: 82961 (1.1%) | Profile: Default

Figure 4.3.7: TCP Packets in Wireshark

19. The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.



```
> Frame 7320673: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_b0:f4:93 (00:0c:29:b0:f4:
> Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
v Transmission Control Protocol, Src Port: 33285, Dst Port: 0, Seq: 67782236, Len: 0
    Source Port: 33285
    Destination Port: 0
    [Stream index: 30762]
    [TCP Segment Len: 0]
    Sequence number: 67782236    (relative sequence number)
    [Next sequence number: 67782236    (relative sequence number)]
  > Acknowledgment number: 715031465
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x000 (<None>)
    Window size value: 512
    [Calculated window size: 512]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x6ecf [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [Timestamps]

0000  00 0c 29 b0 f4 93 00 0c  29 16 01 d1 08 00 45 00   ··)····· )·····E·
0010  00 28 98 b8 00 00 40 06  b9 ed 0a 0a 0a 0d 0a 0a   ·(····@· ········
0020  0a 0a 82 05 00 00 0e 61  d8 3c 2a 9e 83 a9 50 00   ·······a ·<*···P·
0030  02 00 6e cf 00 00 00 00  00 00 00 00               ··n····· ····
```

Figure 4.3.8: TCP packet Stream information

20. This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.

21. Close all open windows and document all the acquired information.

22. Turn off the **Parrot Security** virtual machine.

TASK 4

Create Custom Packets using Nmap to Scan beyond IDS/Firewall

Nmap is a network scanning tool that can be used for sending customized data packets to scan the target host, thus bypassing various security mechanisms such as the IDS/firewall.

Here, we will use Nmap to perform various scanning techniques such as appending custom binary data, appending a custom string, appending random data, randomizing host order, and sending bad checksums to scan the target host beyond the IDS/firewall.

Note: In this task, we are using the **Windows 10** (10.10.10.10) virtual machine as a host machine and the **Windows Server 2016** (10.10.10.16) virtual machine as a target machine.

1. Turn on the **Windows Server 2016** virtual machine and log in the with credentials **Administrator**/**Pa$$w0rd**.

2. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

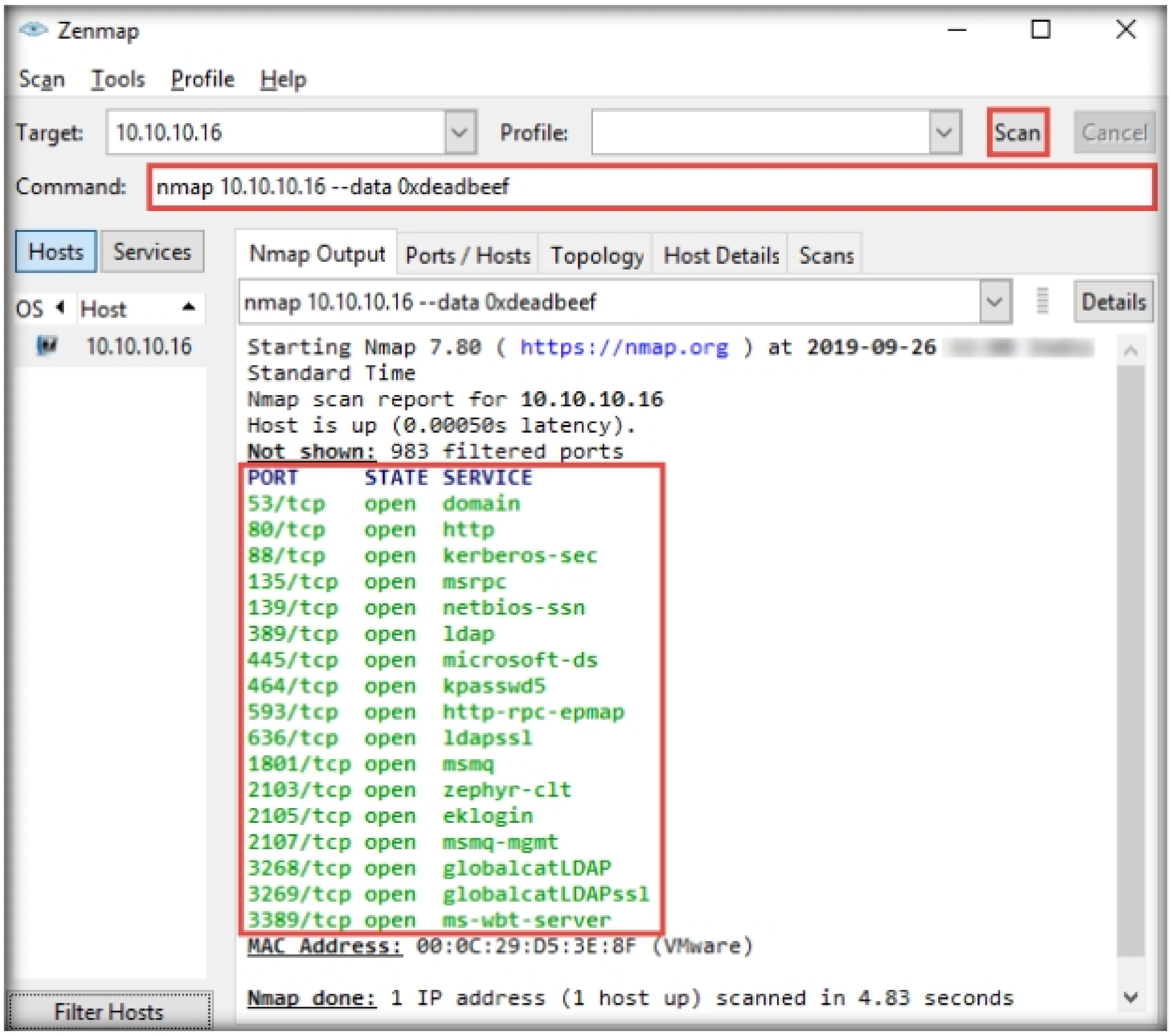
TASK 4.1

Append Custom Binary Data

3. Switch to the **Windows 10** virtual machine and launch **Nmap** by double-clicking on the **Nmap - Zenmap GUI** icon available on **Desktop**.
4. The **Nmap - Zenmap** GUI appears. In the **Command** field, type the command **nmap <Target IP Address> --data 0xdeadbeef** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data <hex string>** (here, **0xdeadbeef**) to send the binary data (o's and 1's) as payloads in the sent packets to scan beyond firewalls.

5. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.



Target: 10.10.10.16

Command: nmap 10.10.10.16 --data 0xdeadbeef

10.10.10.16

```
nmap 10.10.10.16 --data 0xdeadbeef
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-26 [redacted]
Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00050s latency).
Not shown: 983 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
```

Figure 4.4.1: Zenmap scan results for Appending Custom Binary Data

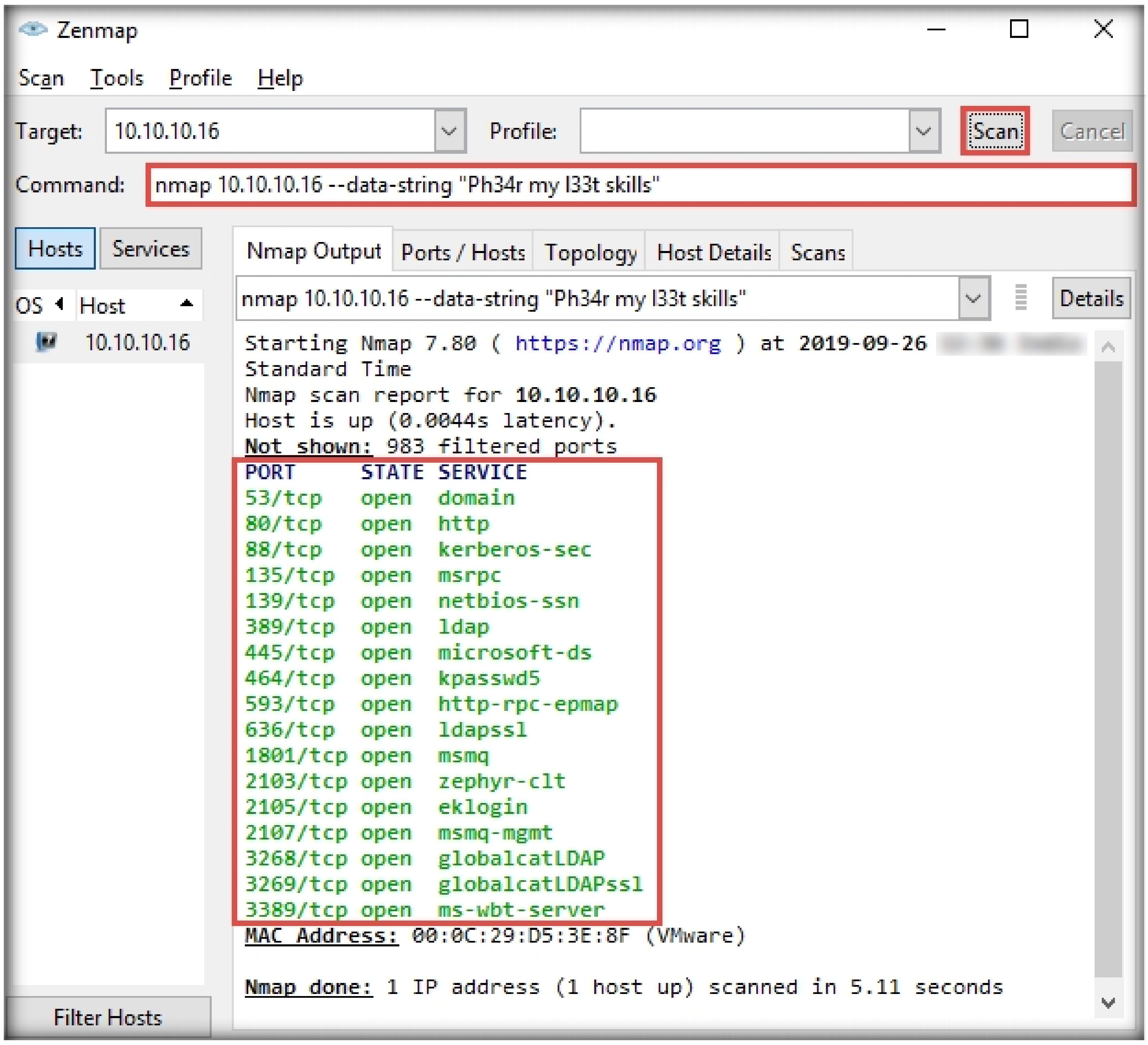
TASK 4.2

Append Custom String

6. In the **Command** field, type the command **nmap <Target IP Address> --data-string "Ph34r my l33t skills"** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-string <string>** (here, "**Ph34r my l33t skills**") to send a regular string as payloads in the sent packets to the target machine for scanning beyond the firewall.

7. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.


Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
Filter Hosts

Target: 10.10.10.16

Command: nmap 10.10.10.16 --data-string "Ph34r my l33t skills"

10.10.10.16

```
nmap 10.10.10.16 --data-string "Ph34r my l33t skills"
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-26 [redacted]
Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.0044s latency).
Not shown: 983 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

Figure 4.4.2: Zenmap scan results for Appending Custom String

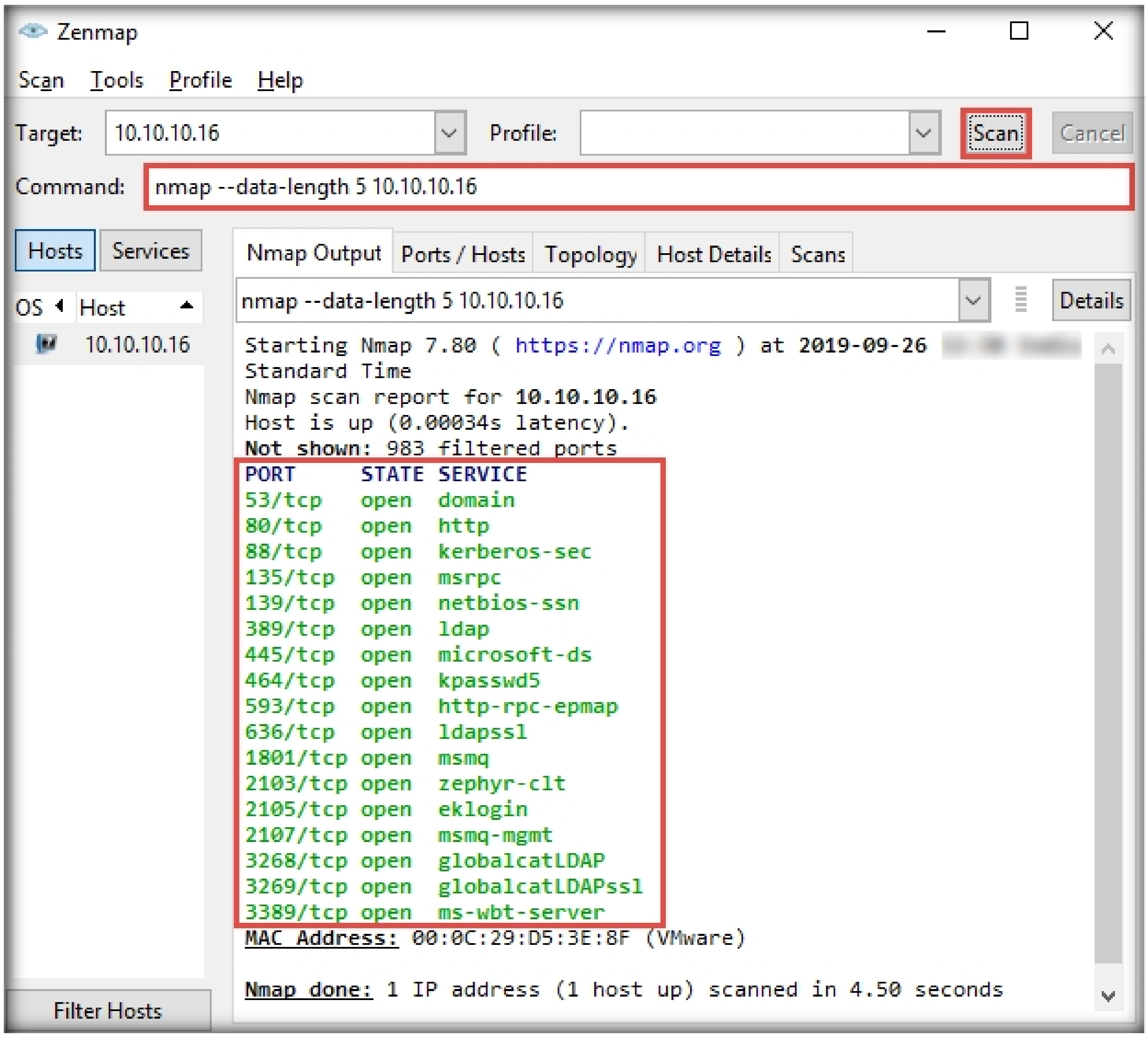
TASK 4.3

Append Random Data

8. In the **Command** field, type the command **nmap --data-length 5 <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-length <len>** (here, **5**) to append the number of random data bytes to most of the packets sent without any protocol-specific payloads.

9. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.


Zenmap
Scan
Tools
Profile
Help
Profile:
Scan
Cancel
Hosts
Services
OS
Host
10.10.10.16
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

Target: 10.10.10.16

Command: nmap --data-length 5 10.10.10.16

```
nmap --data-length 5 10.10.10.16
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-26 [redacted]
Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00034s latency).
Not shown: 983 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

Figure 4.4.3: Zenmap scan results for Appending Random Data

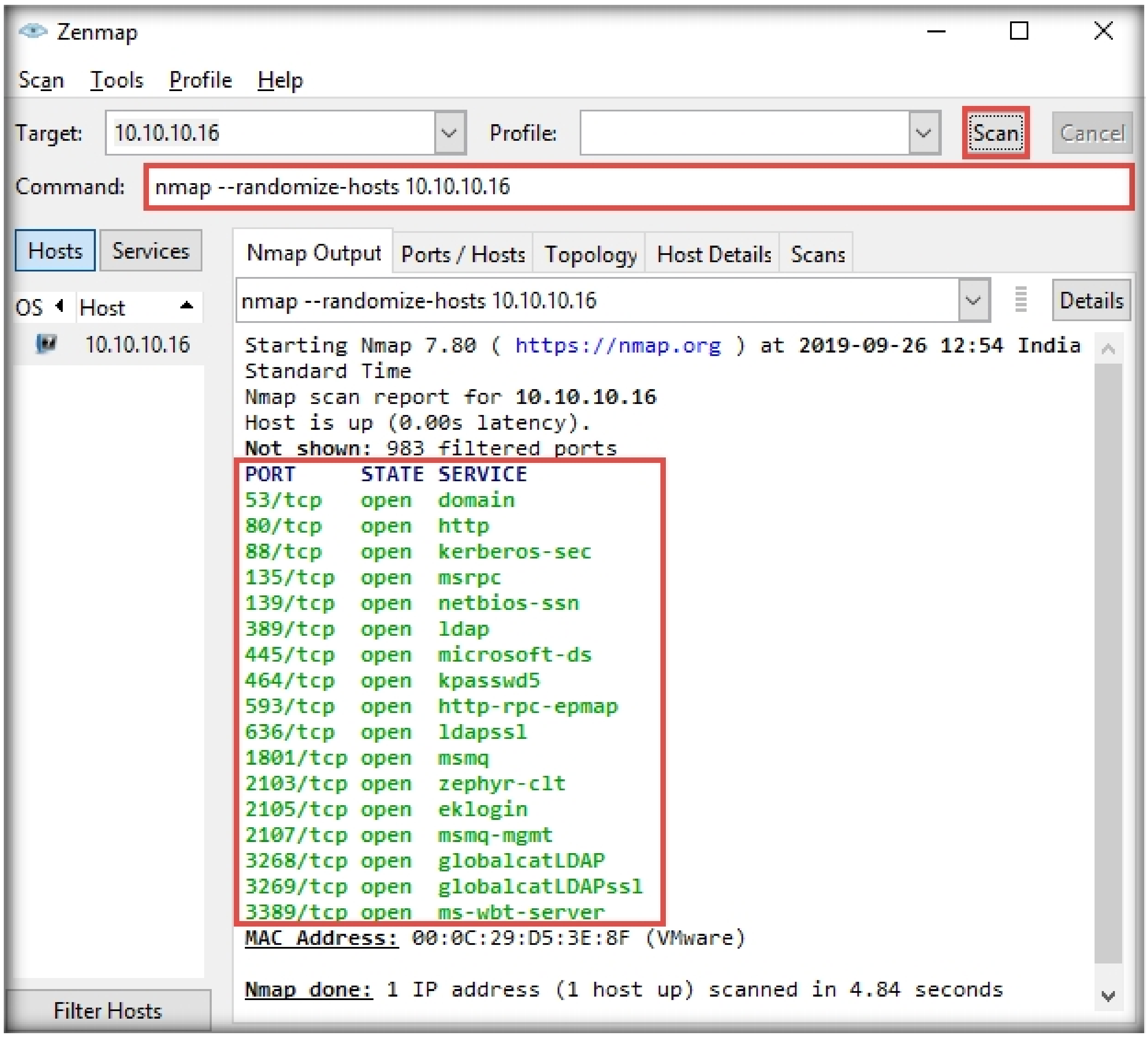
TASK 4.4

Randomizing Host Order

10. In the **Command** field, type the command **nmap --randomize-hosts <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--randomize-hosts** to scan the number of hosts in the target network in random order to scan the intended target that is beyond the firewall.

11. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.


Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap --randomize-hosts 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap --randomize-hosts 10.10.10.16
Details
Filter Hosts

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-26 12:54 India
Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
Not shown: 983 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

Figure 4.4.4: Zenmap scan results for Randomizing Host Order

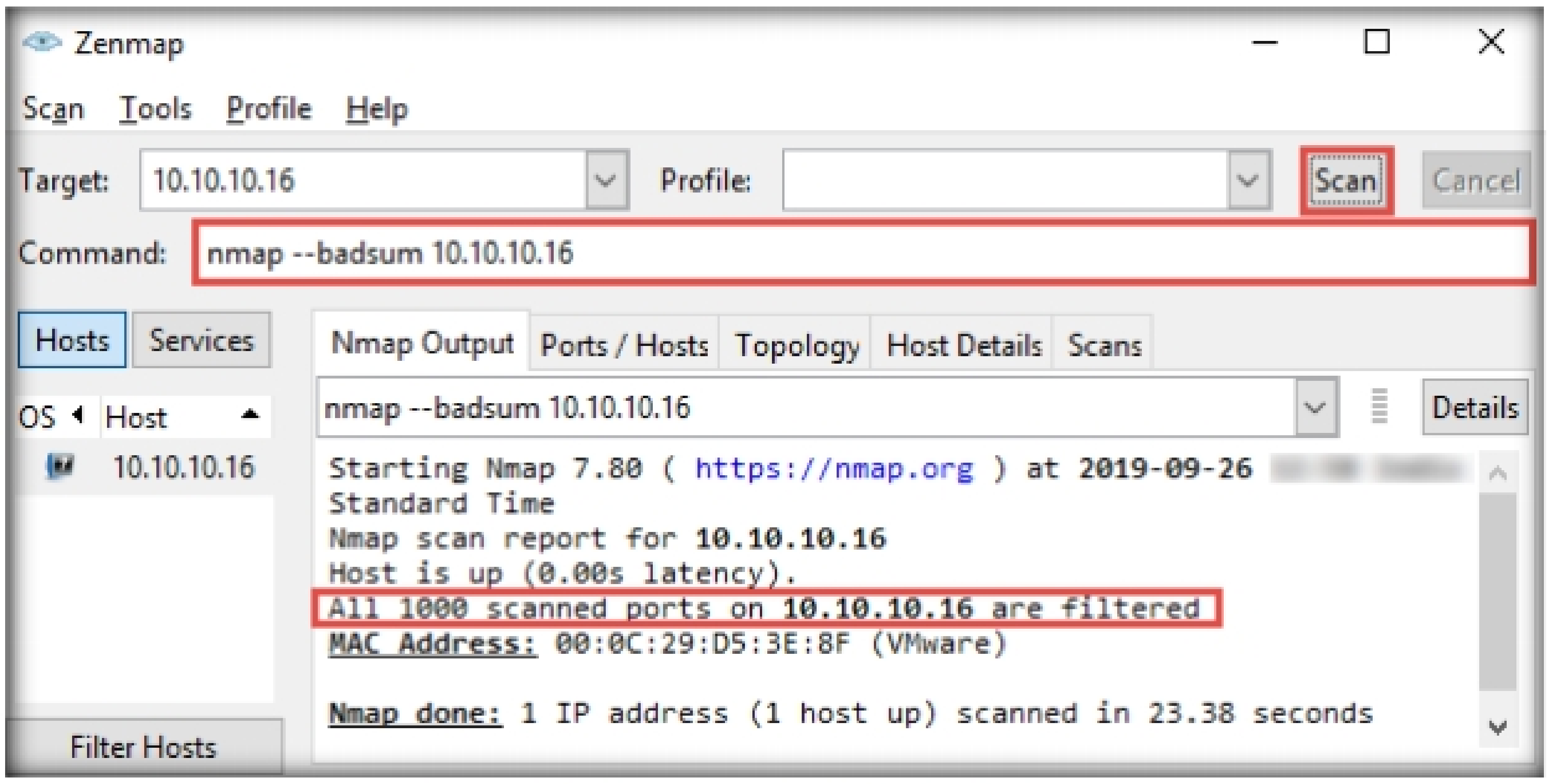
TASK 4.5

Send Bad Checksums

12. In the **Command** field, type the command **nmap --badsum <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--badsum** to send the packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rulesets.

13. The scan results appear, demonstrating that all ports are filtered, indicating that there is no response or the packets are dropped, and thus it can be inferred that the system is configured.


Zenmap
Scan
Tools
Profile
Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap --badsum 10.10.10.16
Hosts
Services
OS
Host
10.10.10.16
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap --badsum 10.10.10.16
Details

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-26 [redacted]
Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.16 are filtered
MAC Address: 00:0C:29:D5:3E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.38 seconds
```

Figure 4.4.5: Zenmap scan results for Bad Checksum

You can also use other packet crafting tools such as **NetScanTools Pro** (https://www.netscantools.com), **Ostinato** (https://www.ostinato.org), and **WAN Killer** (https://www.solarwinds.com) to build custom packets to evade security mechanisms.

14. This concludes the demonstration of creating custom packets using Nmap to scan beyond the IDS and firewall.

15. Close all open windows and document all the acquired information.

16. Turn off the Windows Firewall in the **Windows 10** and **Windows Server 2016** virtual machines by navigating to **Control Panel → System and Security → Windows Firewall → Turn Windows Defender Firewall on or off**.

17. Turn off **Windows Server 2016** virtual machine.

TASK 5

Browse Anonymously using Proxy Switcher

Here, we will use Proxy Switcher to browse the Internet anonymously.

TASK 5.1

Install Proxy Switcher

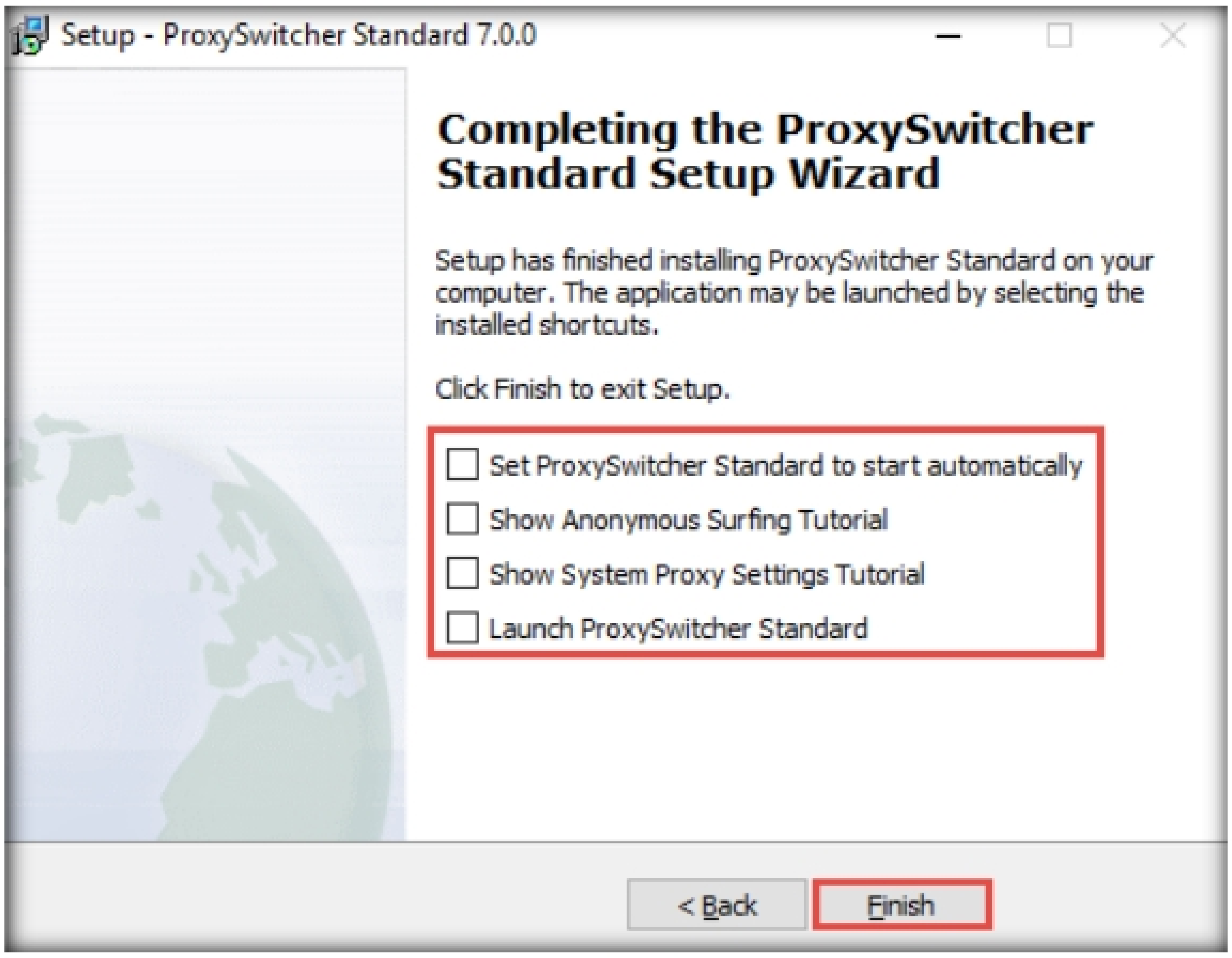
1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher** and double-click **ProxySwitcherStandard.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install Proxy Switcher using all default settings.

3. Once the installation is complete, uncheck all options in the final step of the wizard, and click **Finish**.

Proxy Switcher allows you to surf the Internet anonymously without disclosing the IP address of your system, and helps to access various blocked sites in the organization. It avoids all types of limitations imposed by target sites.


Setup - ProxySwitcher Standard 7.0.0

Completing the ProxySwitcher Standard Setup Wizard

Setup has finished installing ProxySwitcher Standard on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☐ Set ProxySwitcher Standard to start automatically
☐ Show Anonymous Surfing Tutorial
☐ Show System Proxy Settings Tutorial
☐ Launch ProxySwitcher Standard

< Back
Finish

Figure 4.5.1: ProxySwitcher finish wizard

TASK 5.2

Configure Local Proxy in a Web Browser

4. Now, launch the **Firefox** browser.

Note: If a **Default Browser** pop-up appears, click **Not now**.

5. Click the **Open menu** icon in the top-right corner of the browser window and click **Options**.

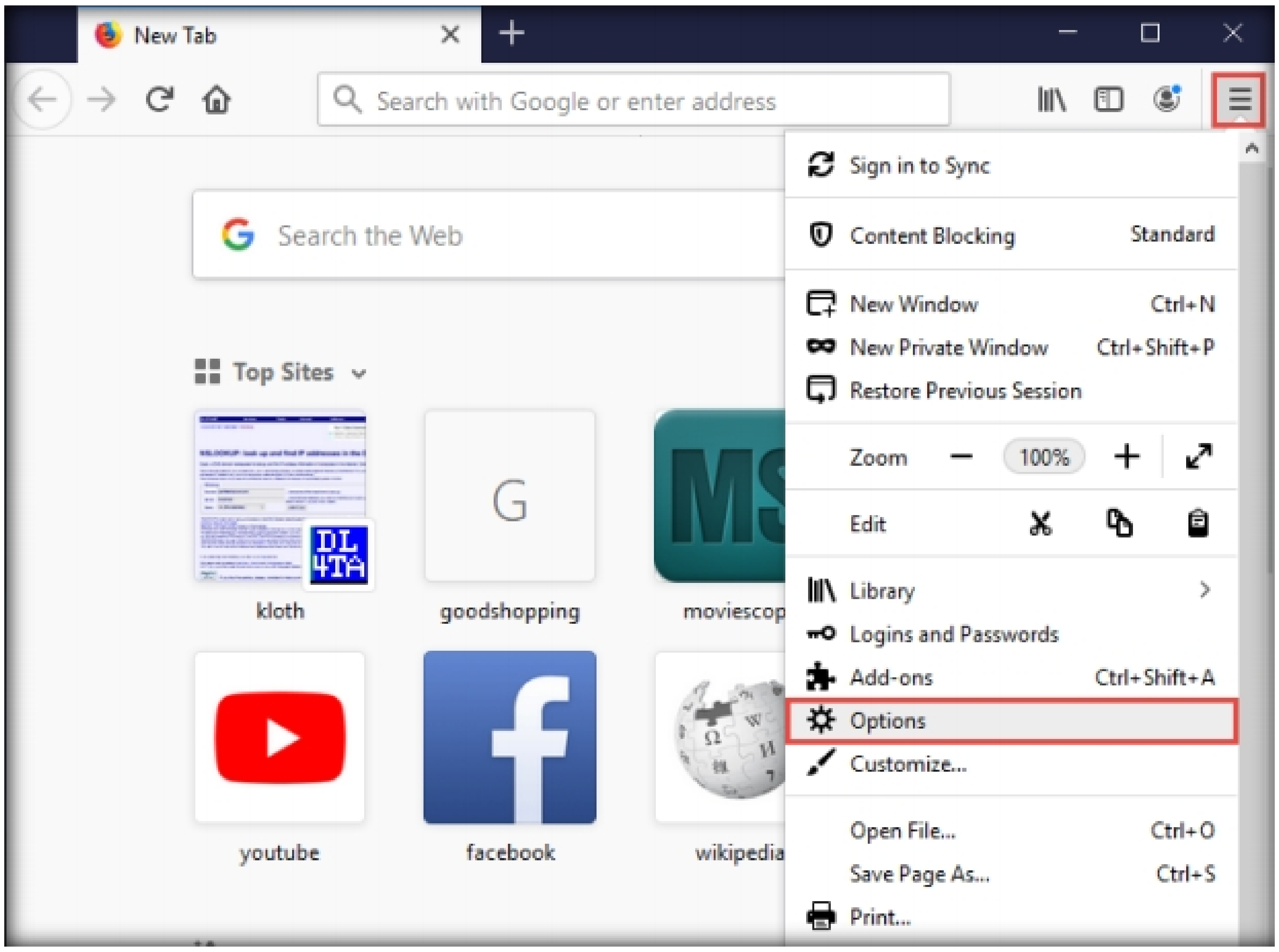
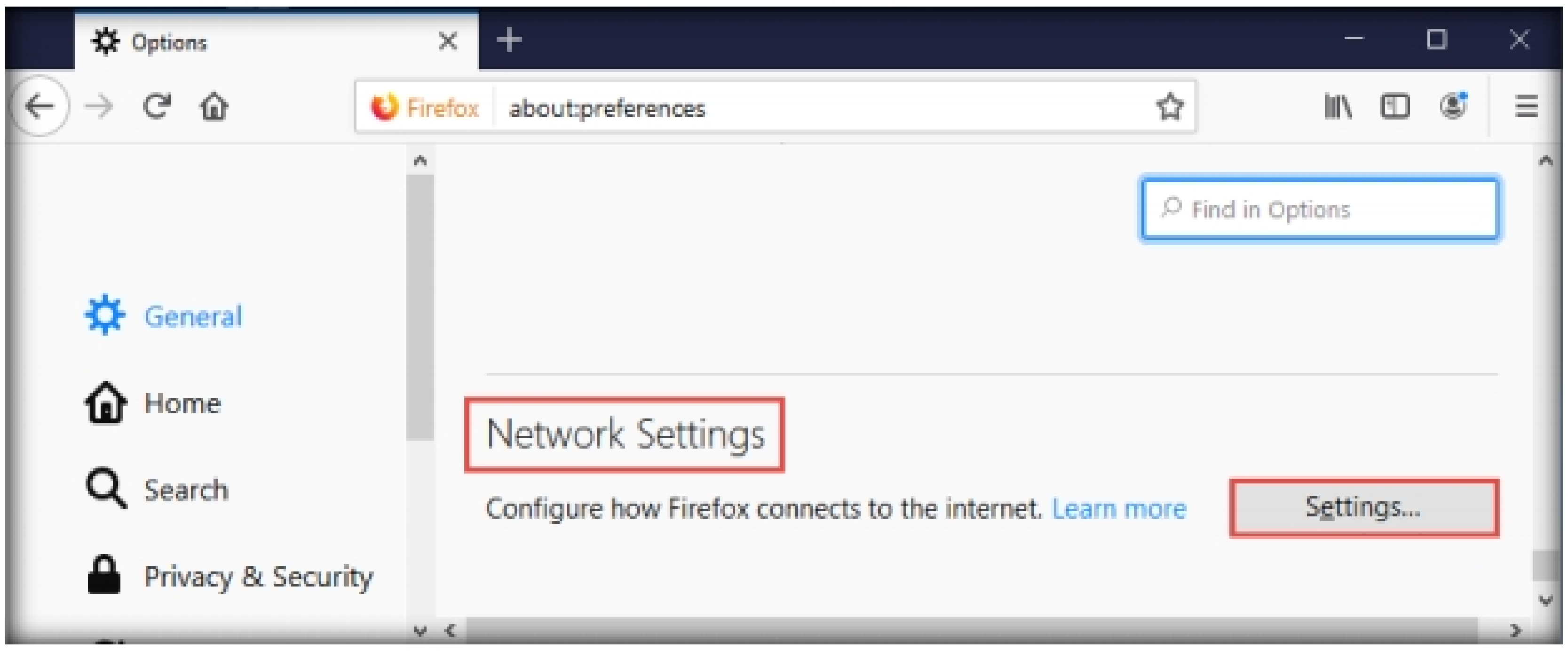

New Tab
Search with Google or enter address
Search the Web
Top Sites
kloth
goodshopping
moviescop
youtube
facebook
wikipedia
Sign in to Sync
Content Blocking Standard
New Window Ctrl+N
New Private Window Ctrl+Shift+P
Restore Previous Session
Zoom 100%
Edit
Library
Logins and Passwords
Add-ons Ctrl+Shift+A
Options
Customize...
Open File... Ctrl+O
Save Page As... Ctrl+S
Print...

Figure 4.5.2: Firefox clicking on Options

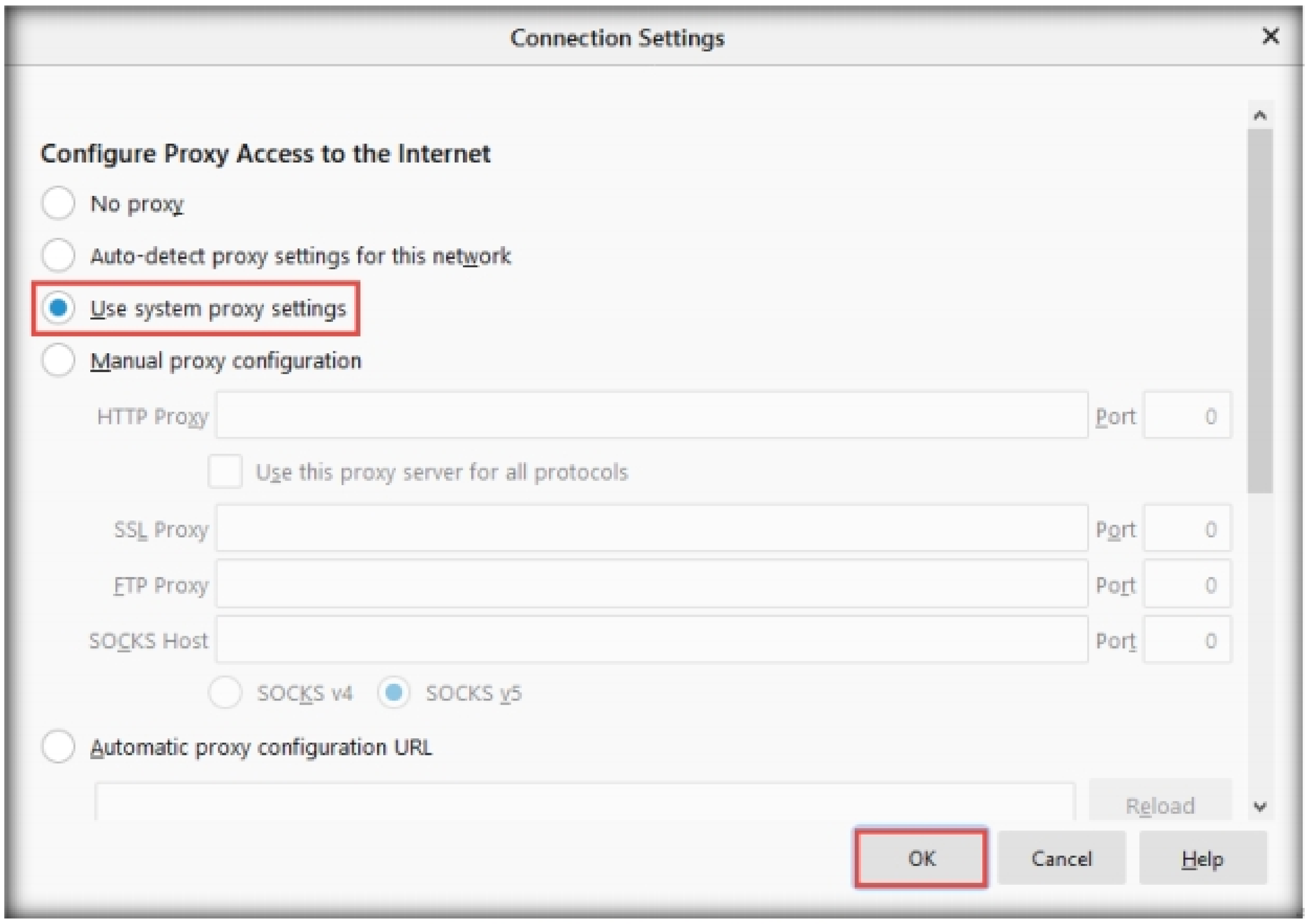
6. In the **Options** wizard, scroll down to the end of the page and click **Settings...** under the **Network Settings** section.


Options
Firefox
about:preferences
Find in Options
General
Home
Search
Privacy & Security
Network Settings
Settings...

Configure how Firefox connects to the internet. Learn more

Figure 4.5.3: Firefox Network Settings

7. The **Connection Settings** window appears; under the **Configure Proxy Access to the Internet** section, ensure that the **Use system proxy settings** radio button is selected. Click **OK** and close the **Firefox** browser window.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
● Use system proxy settings
○ Manual proxy configuration

HTTP Proxy Port 0

☐ Use this proxy server for all protocols

SSL Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload
OK
Cancel
Help

Figure 4.5.4: Firefox Connection Settings

8. Now, click on the **Start** menu and launch **ProxySwitcher Standard** from the applications.

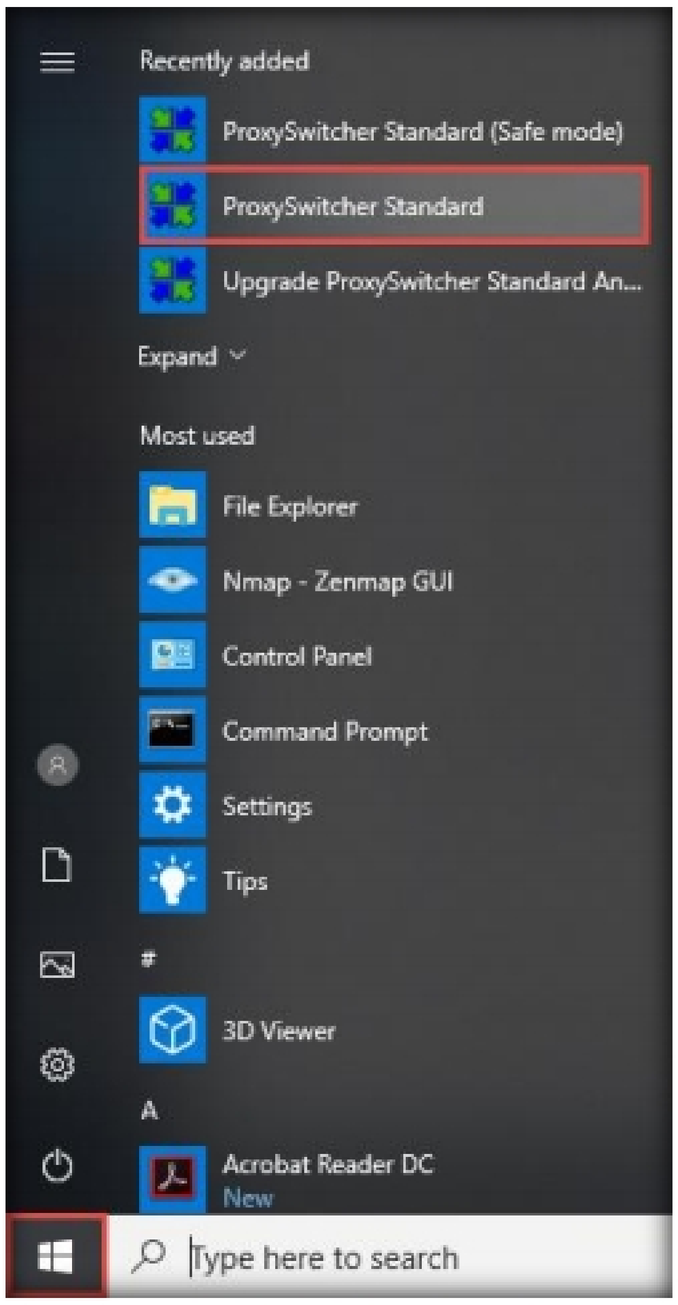

Recently added
ProxySwitcher Standard (Safe mode)
ProxySwitcher Standard
Upgrade ProxySwitcher Standard An...
Expand
Most used
File Explorer
Nmap - Zenmap GUI
Control Panel
Command Prompt
Settings
Tips
#
3D Viewer
A
Acrobat Reader DC
New
Type here to search

Figure 4.5.5: Windows 10 Apps list

9. The **ProxySwitcher Standard** loads, and its icon appears on **Taskbar**.

10. Click the **Taskbar** icon in the bottom-right corner of the desktop and the click **ProxySwitcher Standard** icon to launch the application.

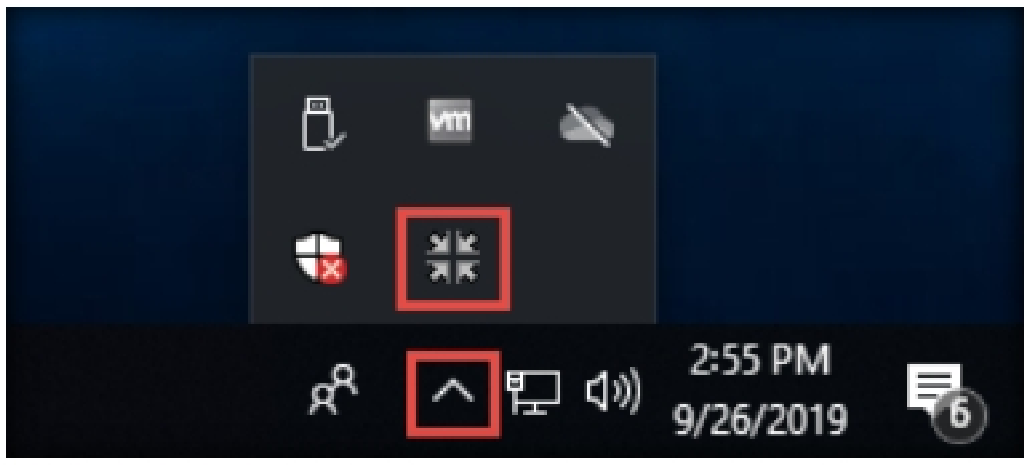

2:55 PM
9/26/2019
6

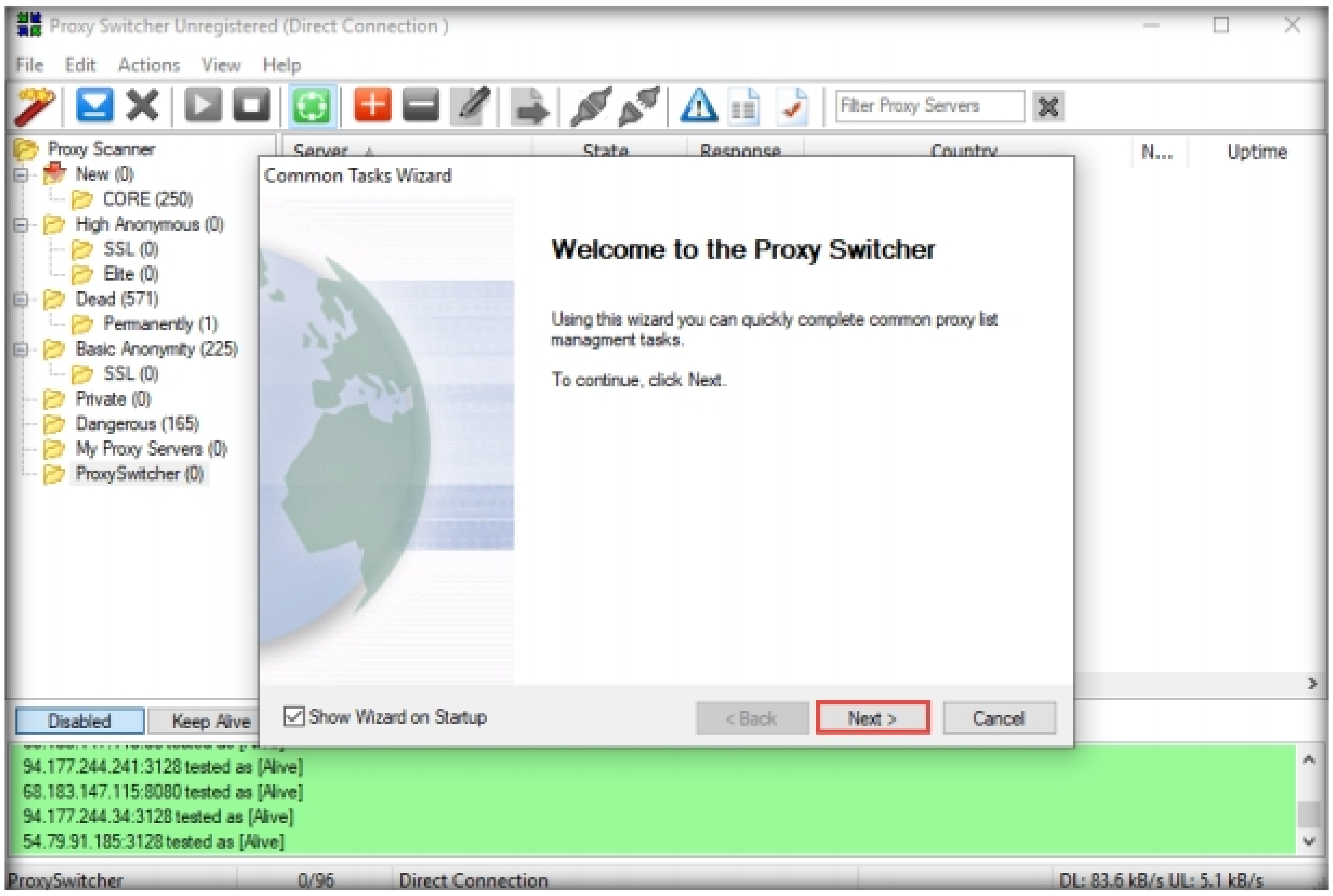
Figure 4.5.6: Selecting ProxySwitcher Standard icon from the taskbar

TASK 5.3

Configure Proxy Switcher

11. The **Please Register** window appears; click the **Start 15 Day Trial** button to proceed.

12. The **Common Tasks Wizard** window appears; under **Welcome to the Proxy Switcher**, click **Next**.


Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (0)
CORE (250)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (571)
Permanently (1)
Basic Anonymity (225)
SSL (0)
Private (0)
Dangerous (165)
My Proxy Servers (0)
ProxySwitcher (0)
Server
State
Response
Country
N...
Uptime
Common Tasks Wizard
Disabled
Keep Alive
☑ Show Wizard on Startup
< Back
Next >
Cancel
ProxySwitcher
0/96
Direct Connection
DL: 83.6 kB/s UL: 5.1 kB/s

Welcome to the Proxy Switcher

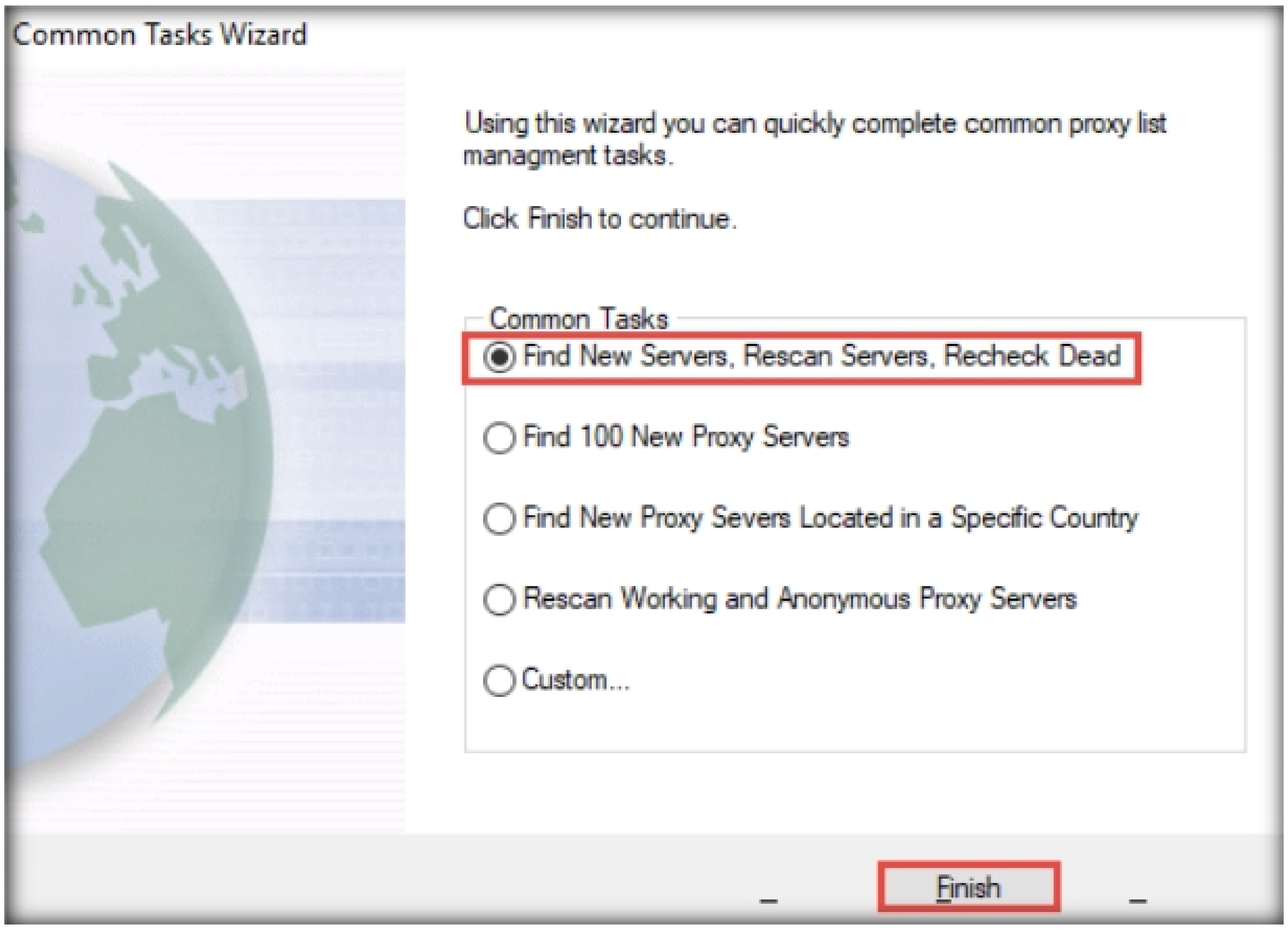
Using this wizard you can quickly complete common proxy list managment tasks.

To continue, click Next.

```
94.177.244.241:3128 tested as [Alive]
68.183.147.115:8080 tested as [Alive]
94.177.244.34:3128 tested as [Alive]
54.79.91.185:3128 tested as [Alive]
```

Figure 4.5.7: Proxy List wizard

13. Ensure that the **Find New Server, Rescan Servers, Recheck Dead** radio button is selected under the **Common Tasks** section, and click **Finish**.


Common Tasks Wizard
Finish

Using this wizard you can quickly complete common proxy list managment tasks.

Click Finish to continue.

Common Tasks

● Find New Servers, Rescan Servers, Recheck Dead

○ Find 100 New Proxy Servers

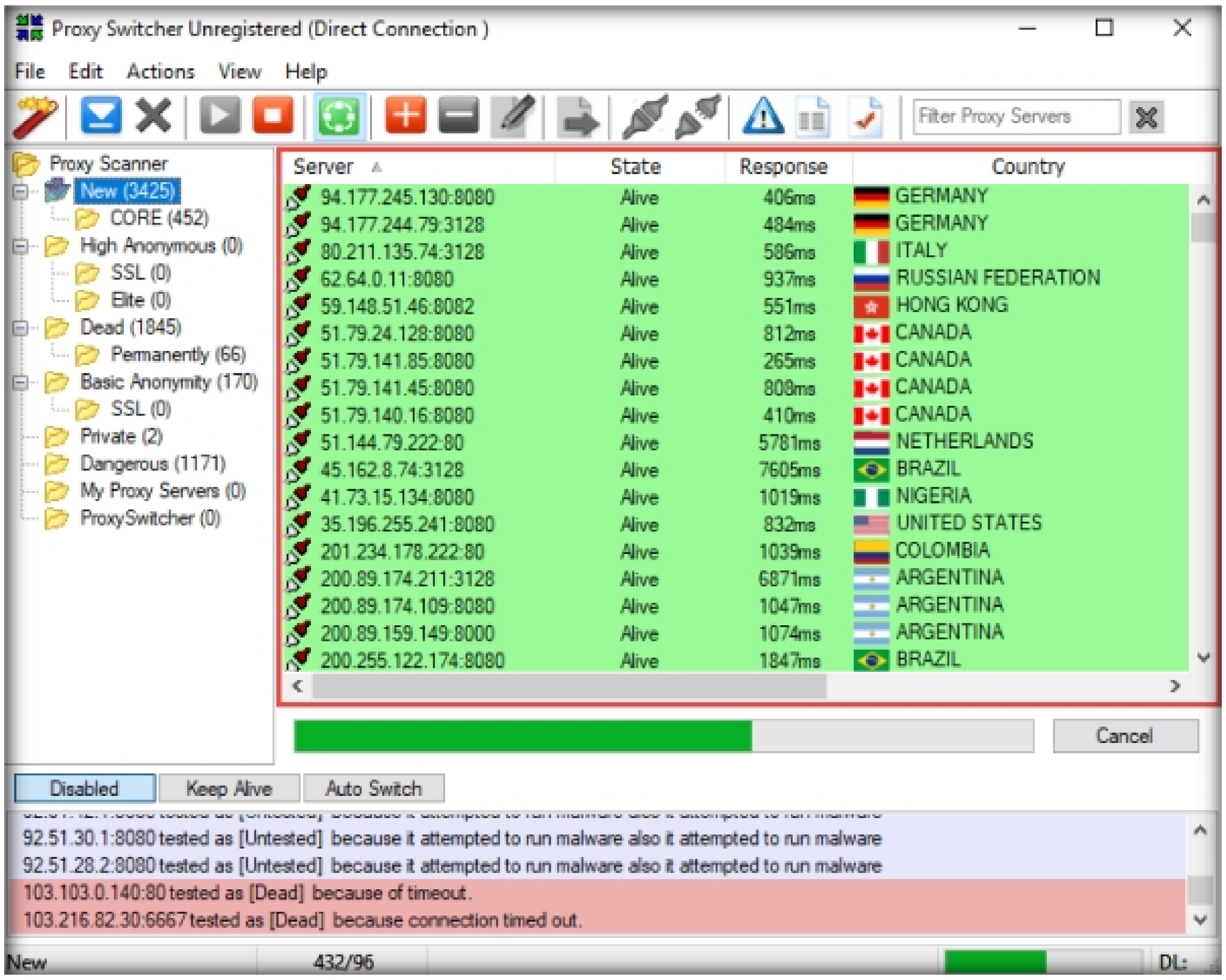
○ Find New Proxy Severs Located in a Specific Country

○ Rescan Working and Anonymous Proxy Servers

○ Custom...

Figure 4.5.8: Selecting common tasks

14. **Proxy Switcher** window appears, showing a list of proxy servers in the right pane, as shown in the following screenshot.


Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (3425)
CORE (452)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (1845)
Permanently (66)
Basic Anonymity (170)
SSL (0)
Private (2)
Dangerous (1171)
My Proxy Servers (0)
ProxySwitcher (0)
Cancel
Disabled
Keep Alive
Auto Switch
New
432/96
DL:

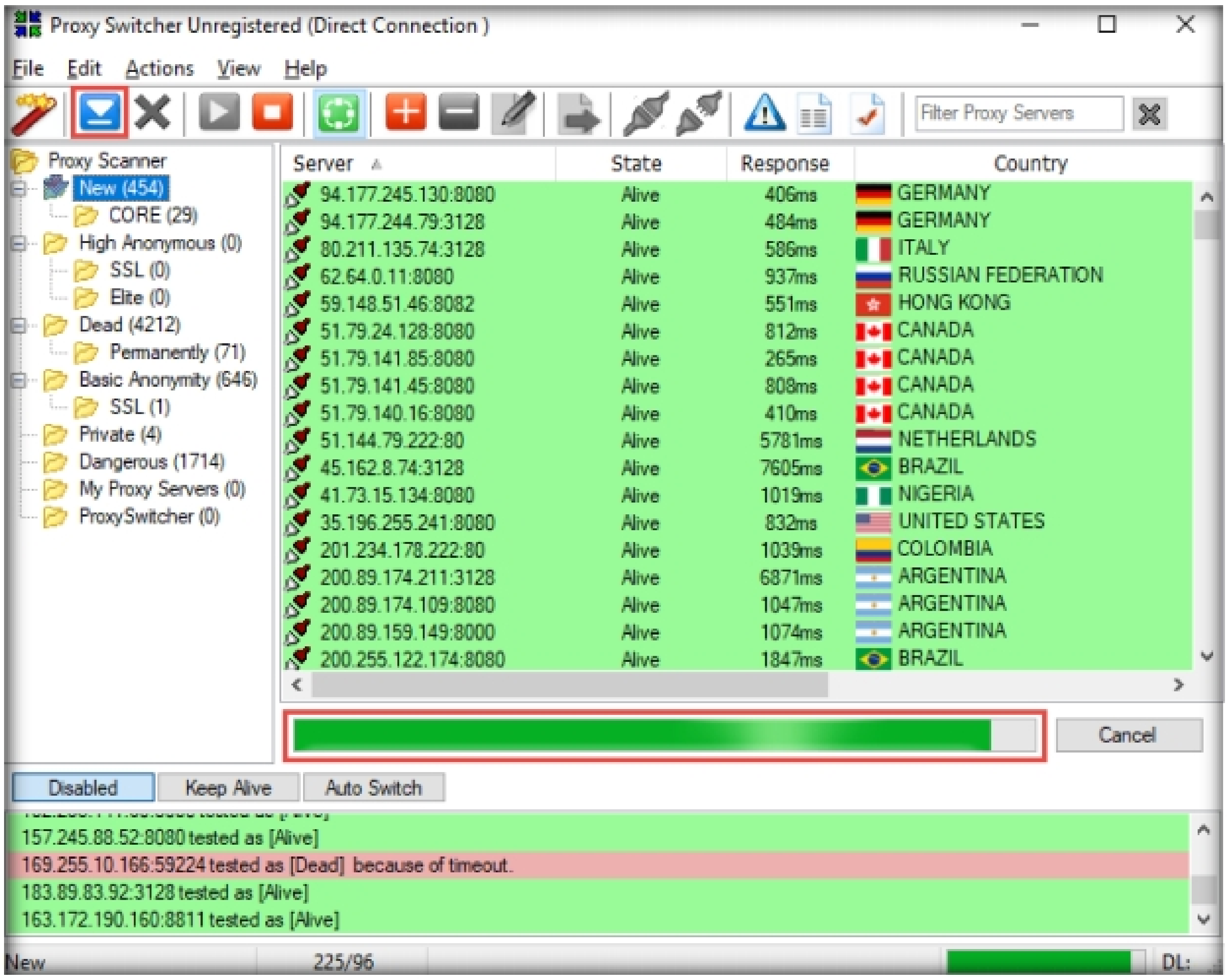
Server	State	Response	Country
94.177.245.130:8080	Alive	406ms	GERMANY
94.177.244.79:3128	Alive	484ms	GERMANY
80.211.135.74:3128	Alive	586ms	ITALY
62.64.0.11:8080	Alive	937ms	RUSSIAN FEDERATION
59.148.51.46:8082	Alive	551ms	HONG KONG
51.79.24.128:8080	Alive	812ms	CANADA
51.79.141.85:8080	Alive	265ms	CANADA
51.79.141.45:8080	Alive	808ms	CANADA
51.79.140.16:8080	Alive	410ms	CANADA
51.144.79.222:80	Alive	5781ms	NETHERLANDS
45.162.8.74:3128	Alive	7605ms	BRAZIL
41.73.15.134:8080	Alive	1019ms	NIGERIA
35.196.255.241:8080	Alive	832ms	UNITED STATES
201.234.178.222:80	Alive	1039ms	COLOMBIA
200.89.174.211:3128	Alive	6871ms	ARGENTINA
200.89.174.109:8080	Alive	1047ms	ARGENTINA
200.89.159.149:8000	Alive	1074ms	ARGENTINA
200.255.122.174:8080	Alive	1847ms	BRAZIL

```
92.51.30.1:8080 tested as [Untested]  because it attempted to run malware also it attempted to run malware
92.51.28.2:8080 tested as [Untested]  because it attempted to run malware also it attempted to run malware
103.103.0.140:80 tested as [Dead]  because of timeout.
103.216.82.30:6667 tested as [Dead]  because connection timed out.
```

Figure 4.5.9: List of downloaded Proxy Servers

Note: The list of proxy servers might vary in your lab environment.

15. Observe the search bar below the server section; once it is completed, click the **Download Proxy Lists** icon ( ) to download the proxy list.


Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (454)
CORE (29)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (4212)
Permanently (71)
Basic Anonymity (646)
SSL (1)
Private (4)
Dangerous (1714)
My Proxy Servers (0)
ProxySwitcher (0)
Cancel
Disabled
Keep Alive
Auto Switch
New
225/96
DL:

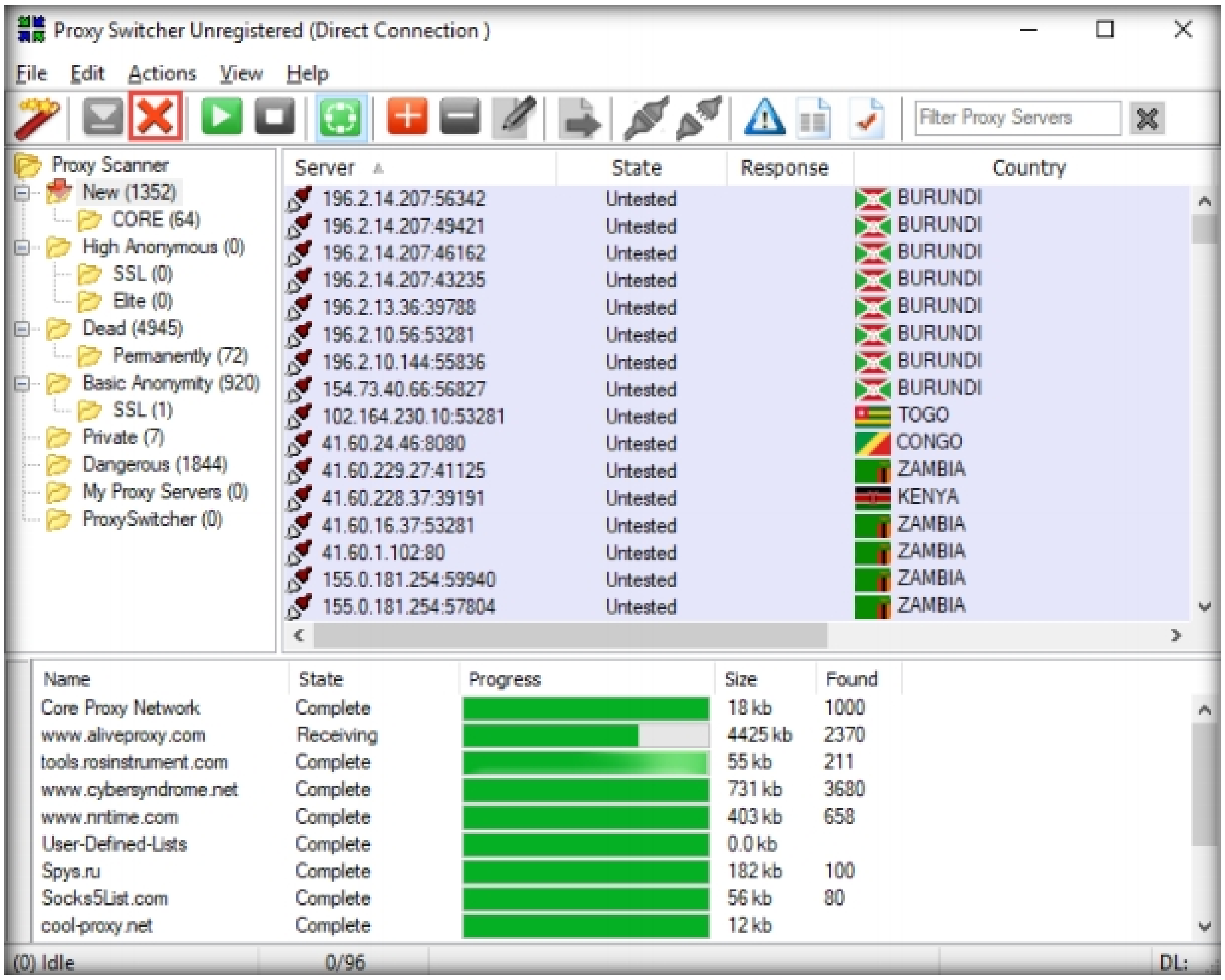
Server	State	Response	Country
94.177.245.130:8080	Alive	406ms	GERMANY
94.177.244.79:3128	Alive	484ms	GERMANY
80.211.135.74:3128	Alive	586ms	ITALY
62.64.0.11:8080	Alive	937ms	RUSSIAN FEDERATION
59.148.51.46:8082	Alive	551ms	HONG KONG
51.79.24.128:8080	Alive	812ms	CANADA
51.79.141.85:8080	Alive	265ms	CANADA
51.79.141.45:8080	Alive	808ms	CANADA
51.79.140.16:8080	Alive	410ms	CANADA
51.144.79.222:80	Alive	5781ms	NETHERLANDS
45.162.8.74:3128	Alive	7605ms	BRAZIL
41.73.15.134:8080	Alive	1019ms	NIGERIA
35.196.255.241:8080	Alive	832ms	UNITED STATES
201.234.178.222:80	Alive	1039ms	COLOMBIA
200.89.174.211:3128	Alive	6871ms	ARGENTINA
200.89.174.109:8080	Alive	1047ms	ARGENTINA
200.89.159.149:8000	Alive	1074ms	ARGENTINA
200.255.122.174:8080	Alive	1847ms	BRAZIL

```
157.245.88.52:8080 tested as [Alive]
169.255.10.166:59224 tested as [Dead]  because of timeout.
183.89.83.92:3128 tested as [Alive]
163.172.190.160:8811 tested as [Alive]
```

Figure 4.5.10: Downing a list of proxy servers

16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.

17. If you have enough downloaded proxy servers, you can click the **Stop Download** (✗) icon to cancel the download.


Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (1352)
CORE (64)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (4945)
Permanently (72)
Basic Anonymity (920)
SSL (1)
Private (7)
Dangerous (1844)
My Proxy Servers (0)
ProxySwitcher (0)
(0) Idle
0/96
DL:

Server	State	Response	Country
196.2.14.207:56342	Untested		BURUNDI
196.2.14.207:49421	Untested		BURUNDI
196.2.14.207:46162	Untested		BURUNDI
196.2.14.207:43235	Untested		BURUNDI
196.2.13.36:39788	Untested		BURUNDI
196.2.10.56:53281	Untested		BURUNDI
196.2.10.144:55836	Untested		BURUNDI
154.73.40.66:56827	Untested		BURUNDI
102.164.230.10:53281	Untested		TOGO
41.60.24.46:8080	Untested		CONGO
41.60.229.27:41125	Untested		ZAMBIA
41.60.228.37:39191	Untested		KENYA
41.60.16.37:53281	Untested		ZAMBIA
41.60.1.102:80	Untested		ZAMBIA
155.0.181.254:59940	Untested		ZAMBIA
155.0.181.254:57804	Untested		ZAMBIA

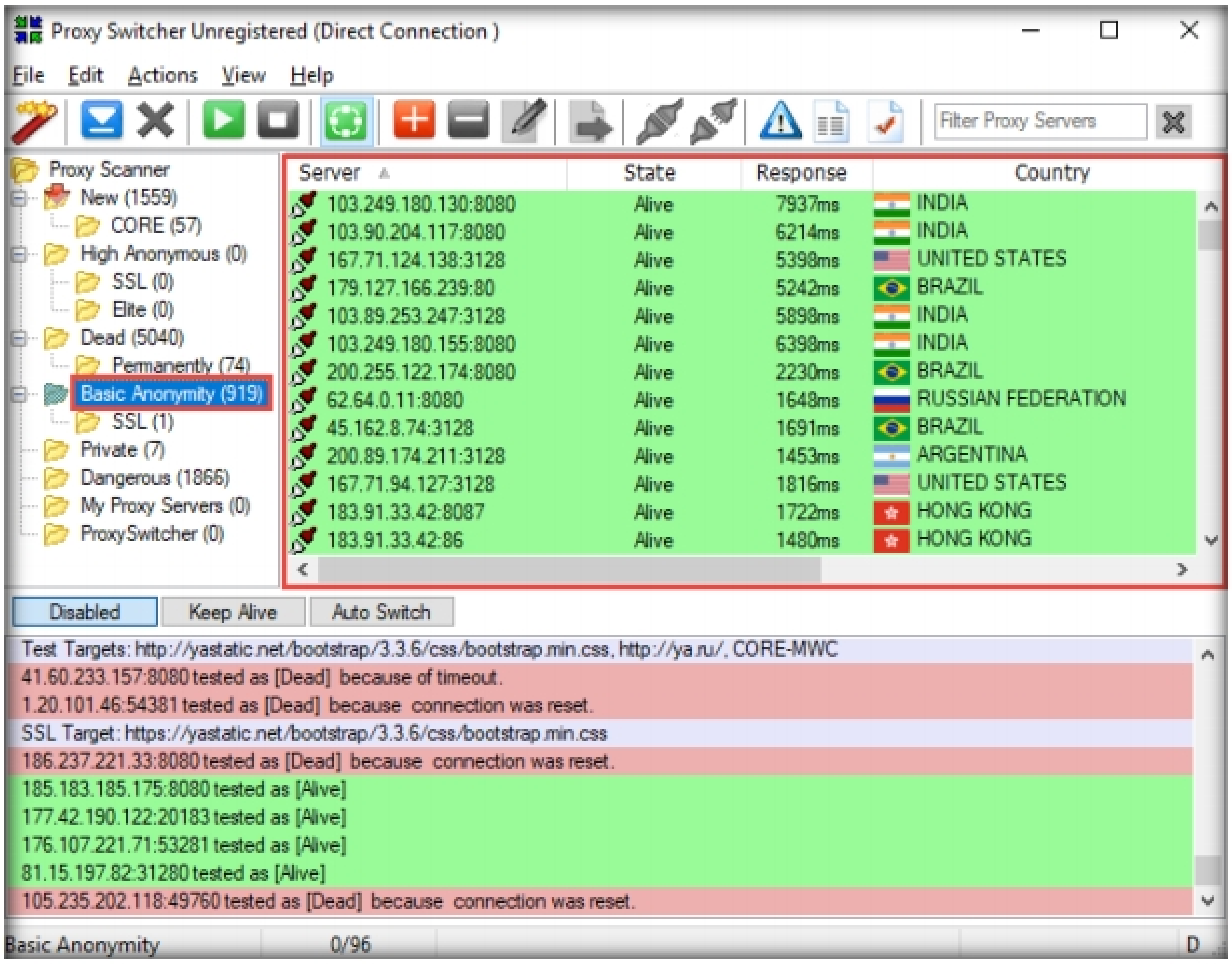
Name	State	Progress	Size	Found
Core Proxy Network	Complete		18 kb	1000
www.aliveproxy.com	Receiving		4425 kb	2370
tools.rosinstrument.com	Complete		55 kb	211
www.cybersyndrome.net	Complete		731 kb	3680
www.nntime.com	Complete		403 kb	658
User-Defined-Lists	Complete		0.0 kb	
Spys.ru	Complete		182 kb	100
Socks5List.com	Complete		56 kb	80
cool-proxy.net	Complete		12 kb	

Figure 4.5.11: Proxies being downloaded

TASK 5.4

Assign Proxies

18. Click the **Basic Anonymity** folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.


Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (1559)
CORE (57)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (5040)
Permanently (74)
Basic Anonymity (919)
SSL (1)
Private (7)
Dangerous (1866)
My Proxy Servers (0)
ProxySwitcher (0)
Disabled
Keep Alive
Auto Switch
Basic Anonymity
0/96
D

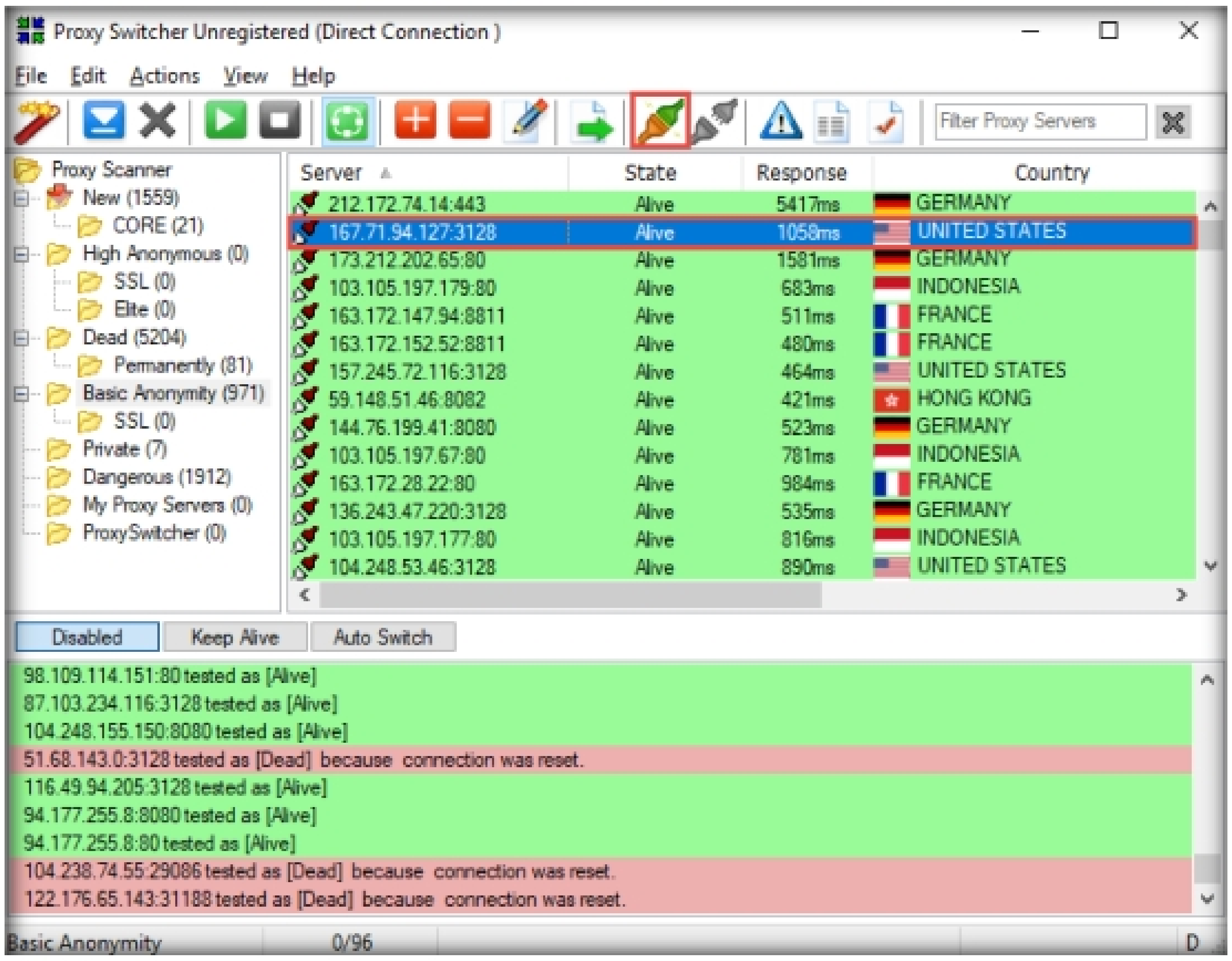
Server	State	Response	Country
103.249.180.130:8080	Alive	7937ms	INDIA
103.90.204.117:8080	Alive	6214ms	INDIA
167.71.124.138:3128	Alive	5398ms	UNITED STATES
179.127.166.239:80	Alive	5242ms	BRAZIL
103.89.253.247:3128	Alive	5898ms	INDIA
103.249.180.155:8080	Alive	6398ms	INDIA
200.255.122.174:8080	Alive	2230ms	BRAZIL
62.64.0.11:8080	Alive	1648ms	RUSSIAN FEDERATION
45.162.8.74:3128	Alive	1691ms	BRAZIL
200.89.174.211:3128	Alive	1453ms	ARGENTINA
167.71.94.127:3128	Alive	1816ms	UNITED STATES
183.91.33.42:8087	Alive	1722ms	HONG KONG
183.91.33.42:86	Alive	1480ms	HONG KONG

```
Test Targets: http://yastatic.net/bootstrap/3.3.6/css/bootstrap.min.css, http://ya.ru/, CORE-MWC
41.60.233.157:8080 tested as [Dead] because of timeout.
1.20.101.46:54381 tested as [Dead] because connection was reset.
SSL Target: https://yastatic.net/bootstrap/3.3.6/css/bootstrap.min.css
186.237.221.33:8080 tested as [Dead] because connection was reset.
185.183.185.175:8080 tested as [Alive]
177.42.190.122:20183 tested as [Alive]
176.107.221.71:53281 tested as [Alive]
81.15.197.82:31280 tested as [Alive]
105.235.202.118:49760 tested as [Dead] because connection was reset.
```

Figure 4.5.12: Searching for alive proxy servers

19. Select one proxy server IP address in the right-hand pane. To switch to the selected proxy server, click the **Switch to Selected Proxy Server** ( ) icon.

Note: The proxy selected in this lab might vary in your lab environment.

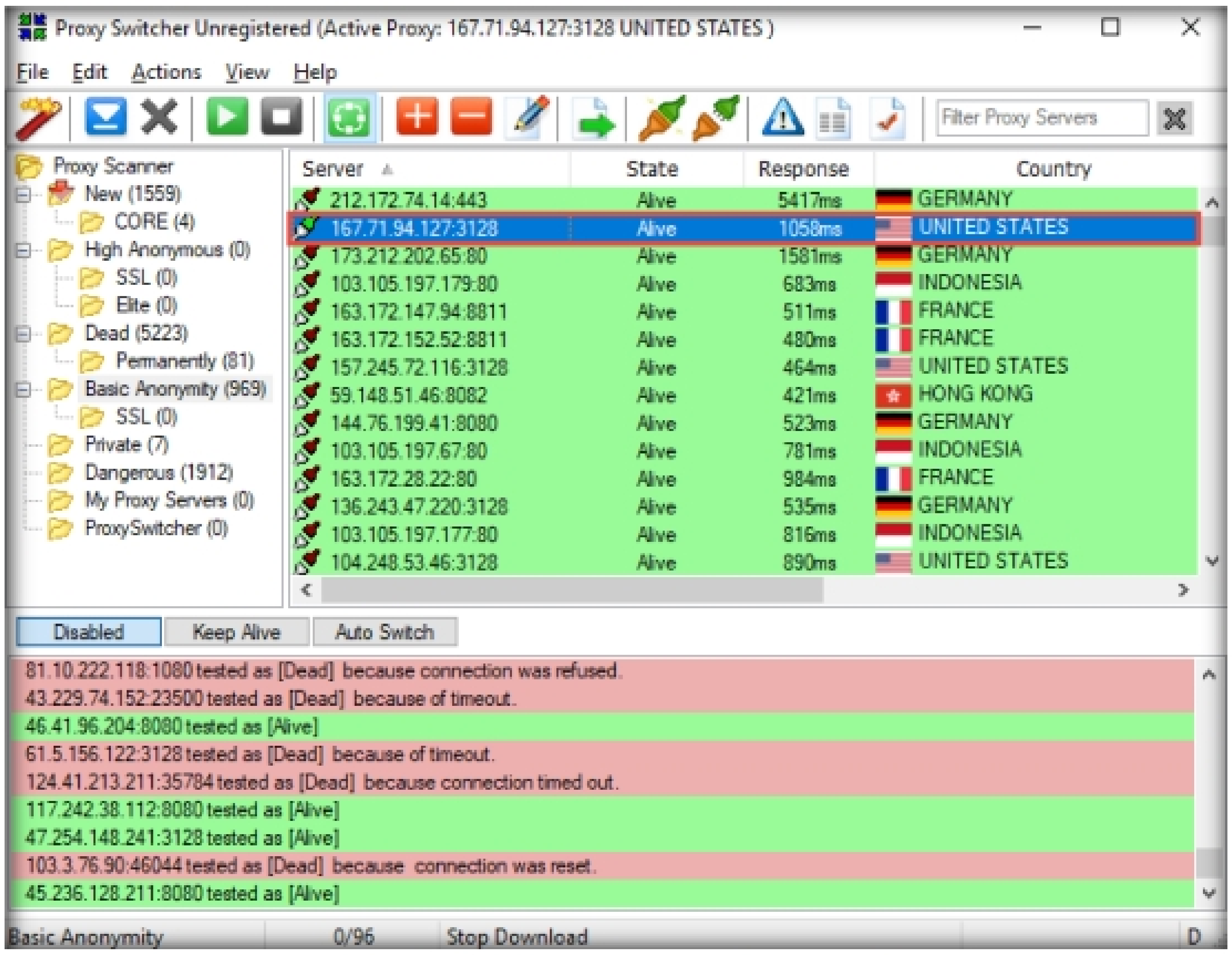

Proxy Switcher Unregistered (Direct Connection)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (1559)
CORE (21)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (5204)
Permanently (81)
Basic Anonymity (971)
SSL (0)
Private (7)
Dangerous (1912)
My Proxy Servers (0)
ProxySwitcher (0)
Disabled
Keep Alive
Auto Switch
Basic Anonymity
0/96
D

Server	State	Response	Country
212.172.74.14:443	Alive	5417ms	GERMANY
167.71.94.127:3128	Alive	1058ms	UNITED STATES
173.212.202.65:80	Alive	1581ms	GERMANY
103.105.197.179:80	Alive	683ms	INDONESIA
163.172.147.94:8811	Alive	511ms	FRANCE
163.172.152.52:8811	Alive	480ms	FRANCE
157.245.72.116:3128	Alive	464ms	UNITED STATES
59.148.51.46:8082	Alive	421ms	HONG KONG
144.76.199.41:8080	Alive	523ms	GERMANY
103.105.197.67:80	Alive	781ms	INDONESIA
163.172.28.22:80	Alive	984ms	FRANCE
136.243.47.220:3128	Alive	535ms	GERMANY
103.105.197.177:80	Alive	816ms	INDONESIA
104.248.53.46:3128	Alive	890ms	UNITED STATES

```
98.109.114.151:80 tested as [Alive]
87.103.234.116:3128 tested as [Alive]
104.248.155.150:8080 tested as [Alive]
51.68.143.0:3128 tested as [Dead]  because  connection was reset.
116.49.94.205:3128 tested as [Alive]
94.177.255.8:8080 tested as [Alive]
94.177.255.8:80 tested as [Alive]
104.238.74.55:29086 tested as [Dead]  because  connection was reset.
122.176.65.143:31188 tested as [Dead]  because  connection was reset.
```

Figure 4.5.13: Selecting a proxy server

20. When the proxy server is connected, it will show the connection icon as .


Proxy Switcher Unregistered (Active Proxy: 167.71.94.127:3128 UNITED STATES)
File
Edit
Actions
View
Help
Filter Proxy Servers
Proxy Scanner
New (1559)
CORE (4)
High Anonymous (0)
SSL (0)
Elite (0)
Dead (5223)
Permanently (81)
Basic Anonymity (969)
SSL (0)
Private (7)
Dangerous (1912)
My Proxy Servers (0)
ProxySwitcher (0)
Disabled
Keep Alive
Auto Switch
Basic Anonymity
0/96
Stop Download
D

Server	State	Response	Country
212.172.74.14:443	Alive	5417ms	GERMANY
167.71.94.127:3128	Alive	1058ms	UNITED STATES
173.212.202.65:80	Alive	1581ms	GERMANY
103.105.197.179:80	Alive	683ms	INDONESIA
163.172.147.94:8811	Alive	511ms	FRANCE
163.172.152.52:8811	Alive	480ms	FRANCE
157.245.72.116:3128	Alive	464ms	UNITED STATES
59.148.51.46:8082	Alive	421ms	HONG KONG
144.76.199.41:8080	Alive	523ms	GERMANY
103.105.197.67:80	Alive	781ms	INDONESIA
163.172.28.22:80	Alive	984ms	FRANCE
136.243.47.220:3128	Alive	535ms	GERMANY
103.105.197.177:80	Alive	816ms	INDONESIA
104.248.53.46:3128	Alive	890ms	UNITED STATES

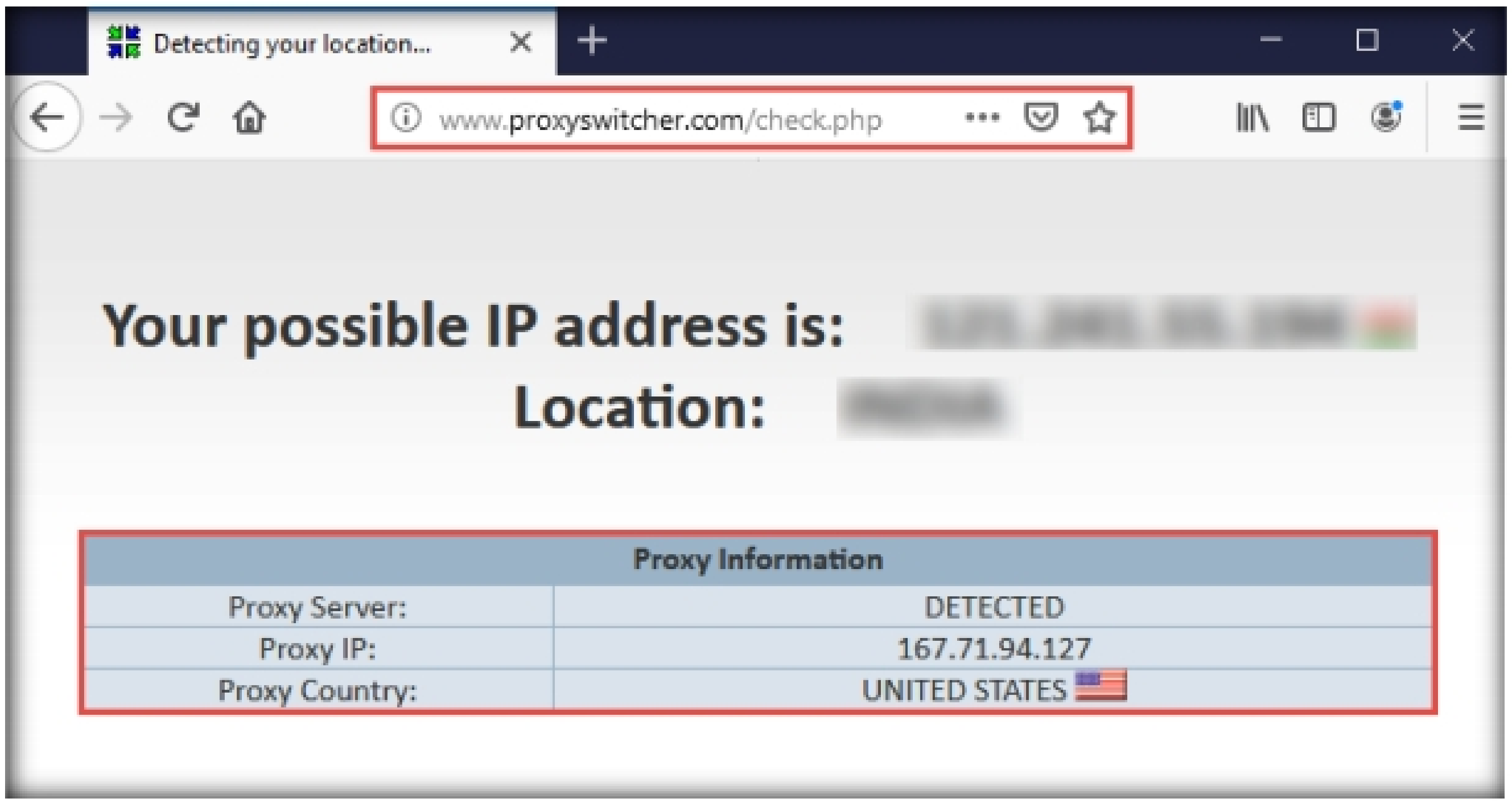
```
81.10.222.118:1080 tested as [Dead]  because connection was refused.
43.229.74.152:23500 tested as [Dead]  because of timeout.
46.41.96.204:8080 tested as [Alive]
61.5.156.122:3128 tested as [Dead]  because of timeout.
124.41.213.211:35784 tested as [Dead]  because connection timed out.
117.242.38.112:8080 tested as [Alive]
47.254.148.241:3128 tested as [Alive]
103.3.76.90:46044 tested as [Dead]  because  connection was reset.
45.236.128.211:8080 tested as [Alive]
```

Figure 4.5.14: Proxy server successfully connected

TASK 5.5

Test Proxies

21. Launch the **Mozilla Firefox** web browser and enter the URL **http://www.proxyswitcher.com/check.php** to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:


Detecting your location...
www.proxyswitcher.com/check.php

Your possible IP address is: [redacted]

Location: [redacted]

Proxy Information	
Proxy Server:	DETECTED
Proxy IP:	167.71.94.127
Proxy Country:	UNITED STATES

Figure 4.5.15: Detected Proxy Server

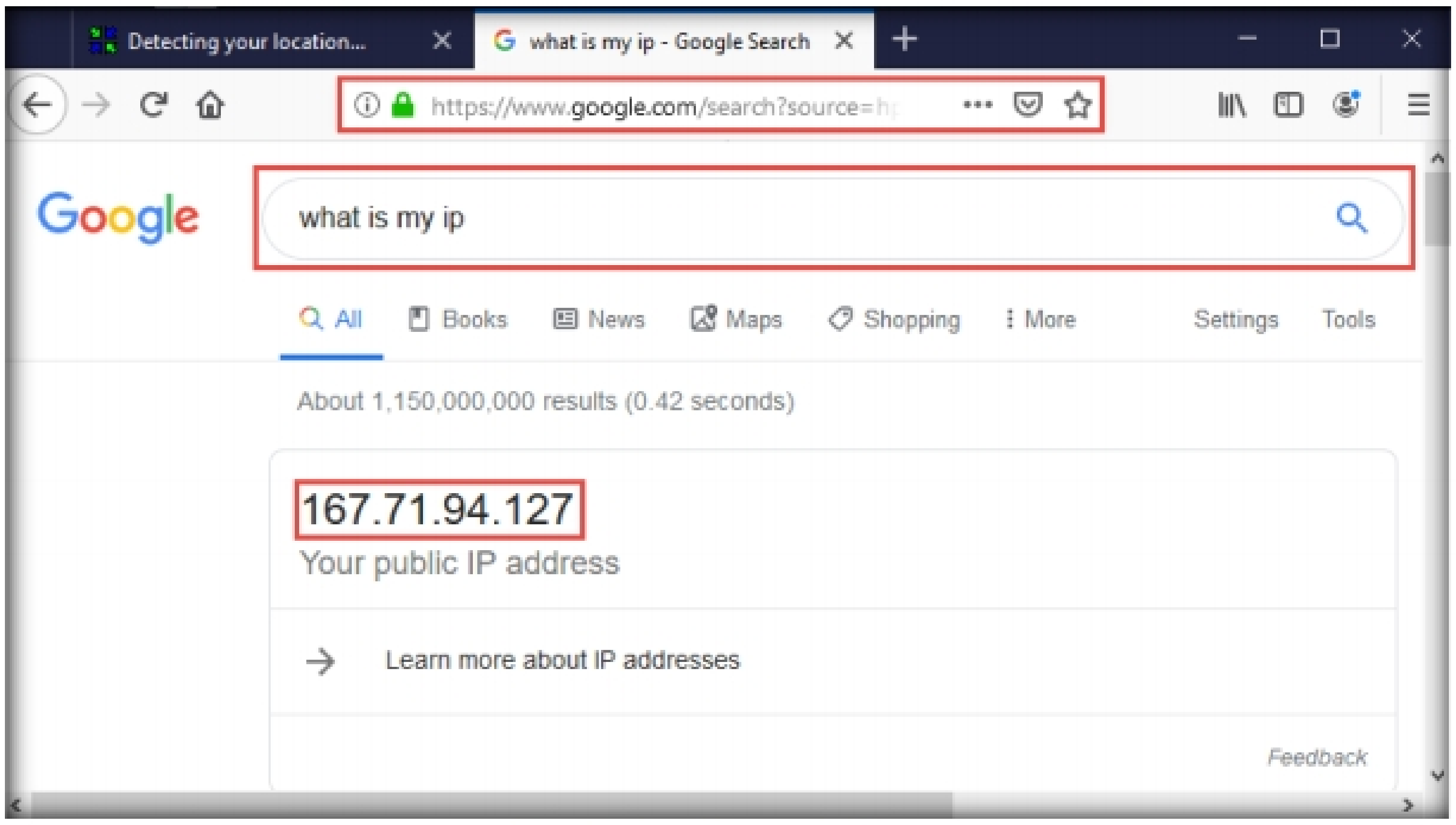
Note: The information displayed above may differ in your lab environment.

22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 19**.

23. To ensure that the proxy is assigned, open a new tab and browse **https://www.google.com/**. In the search field, type **What is my ip** and press **Enter**.

24. The proxy IP address (**167.71.94.127**) is displayed, which infers that the legitimate address is masked and the proxy is in use.

Note: The displayed IP address might differ in your lab environment.


Detecting your location...
what is my ip - Google Search
https://www.google.com/search?source=h
Google
All
Books
News
Maps
Shopping
More
Settings
Tools
Feedback

what is my ip

About 1,150,000,000 results (0.42 seconds)

167.71.94.127

Your public IP address

Learn more about IP addresses

Figure 4.5.16: Testing your IP address

25. Open a new tab in your **web browser** and surf anonymously using this proxy.

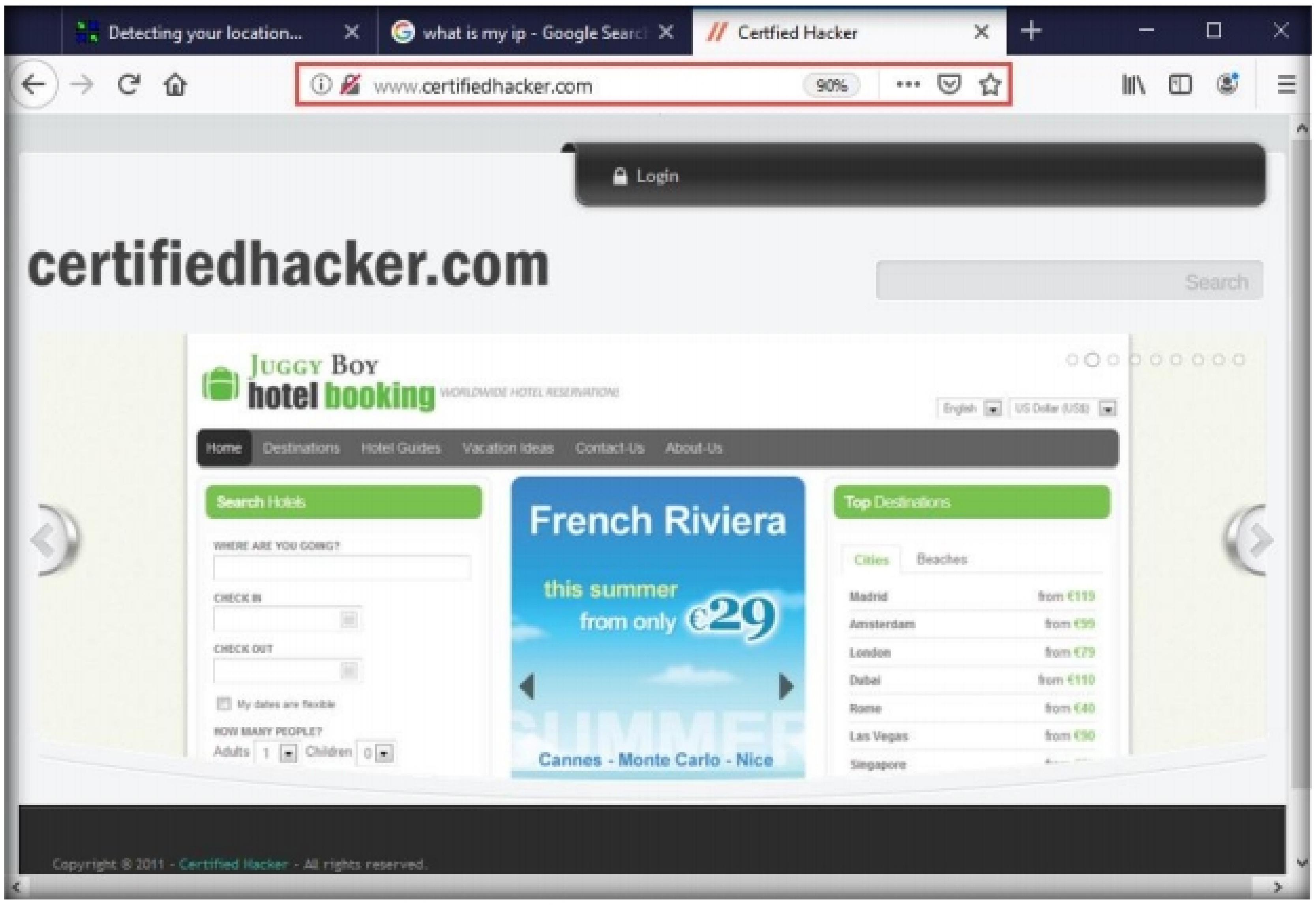

Detecting your location...
what is my ip - Google Search
Certfied Hacker
www.certifiedhacker.com
90%
Login
certifiedhacker.com
Search
Juggy Boy hotel booking
Home
Destinations
Hotel Guides
Vacation Ideas
Contact-Us
About-Us
Search Hotels
French Riviera
this summer from only €29
Cannes - Monte Carlo - Nice
Top Destinations
Copyright © 2011 - Certified Hacker - All rights reserved.

Figure 4.5.17: Surfing internet using Proxy server

26. This concludes the demonstration of anonymously surfing the Internet using Proxy Switcher.

27. Close all open windows and document all the acquired information.

28. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall the **Proxy Switcher** application

TASK 6

Browse Anonymously using CyberGhost VPN

Here, we will use CyberGhost VPN to browse the Internet anonymously.

TASK 6.1

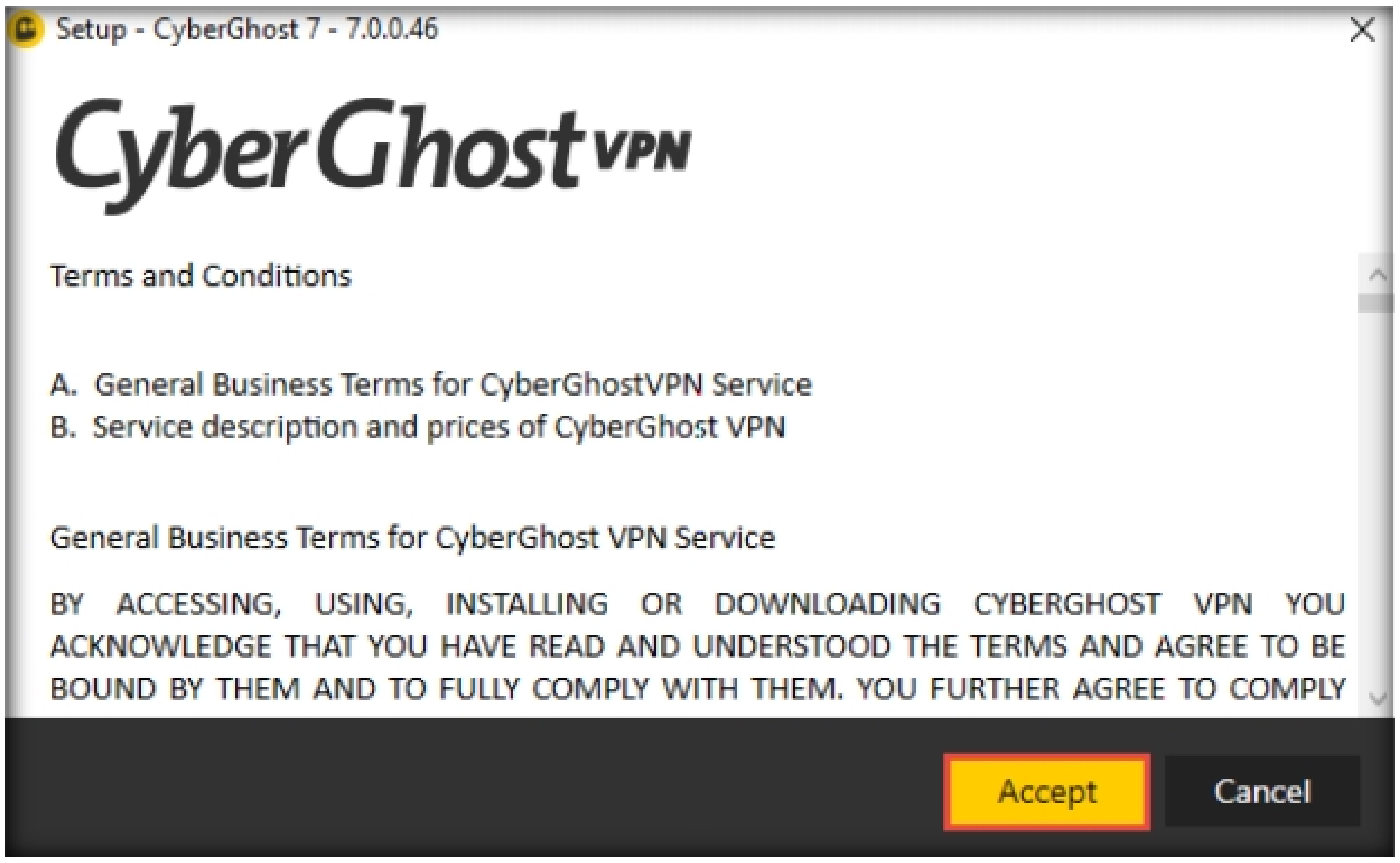
Install CyberGhost VPN

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN** and double-click **cgsetup_en_NMKh64apsGD93kapeBUc.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

CyberGhost VPN hides your IP and replaces it with one of their choice, thereby allowing you to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

2. **Downloading CyberGhost installer...** appears; once the **CyberGhost Setup** window appears, click **Accept**.



Terms and Conditions

A. General Business Terms for CyberGhostVPN Service
B. Service description and prices of CyberGhost VPN

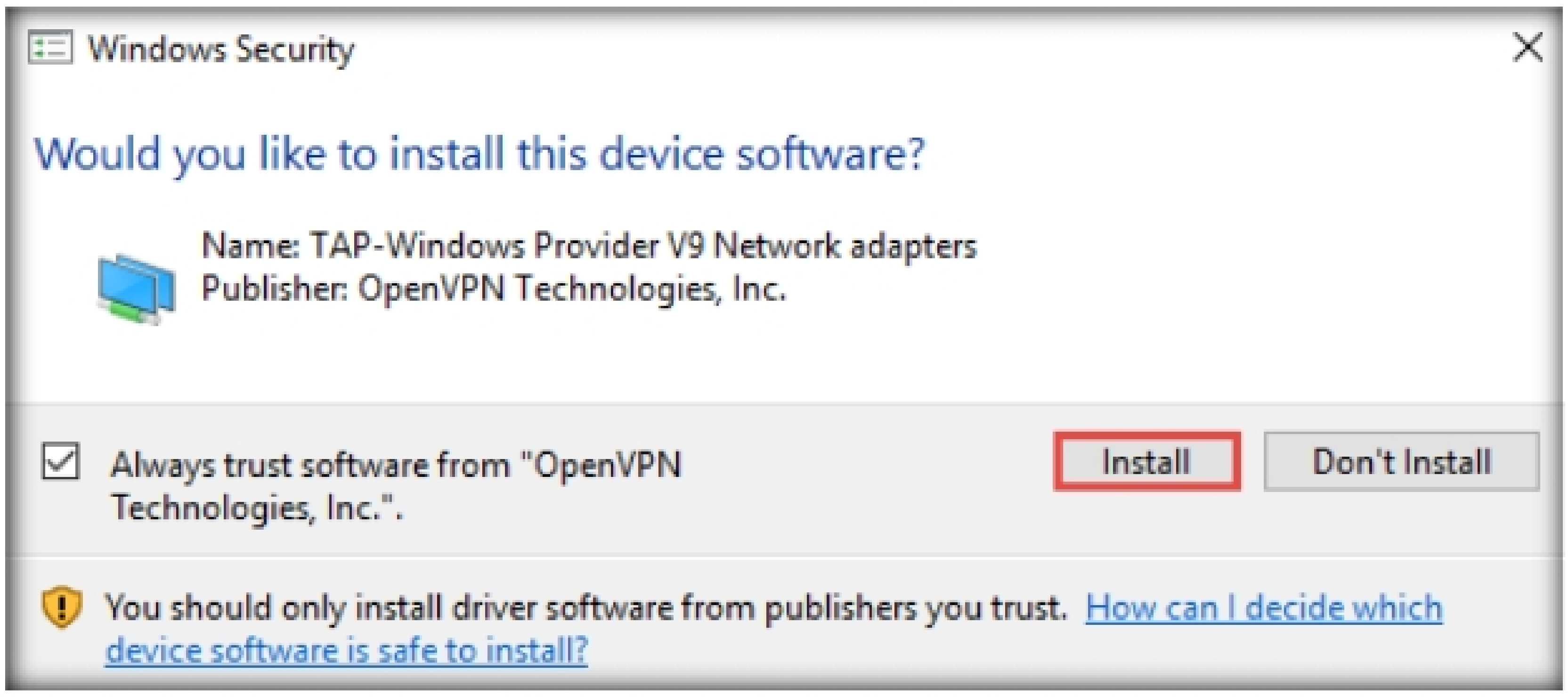
General Business Terms for CyberGhost VPN Service

BY ACCESSING, USING, INSTALLING OR DOWNLOADING CYBERGHOST VPN YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THE TERMS AND AGREE TO BE BOUND BY THEM AND TO FULLY COMPLY WITH THEM. YOU FURTHER AGREE TO COMPLY

Figure 4.6.1: CyberGhost Setup window

3. Follow the installation steps to install **CyberGhost**.

4. If a **Windows Security** pop-up appears, click **Install**.



Would you like to install this device software?

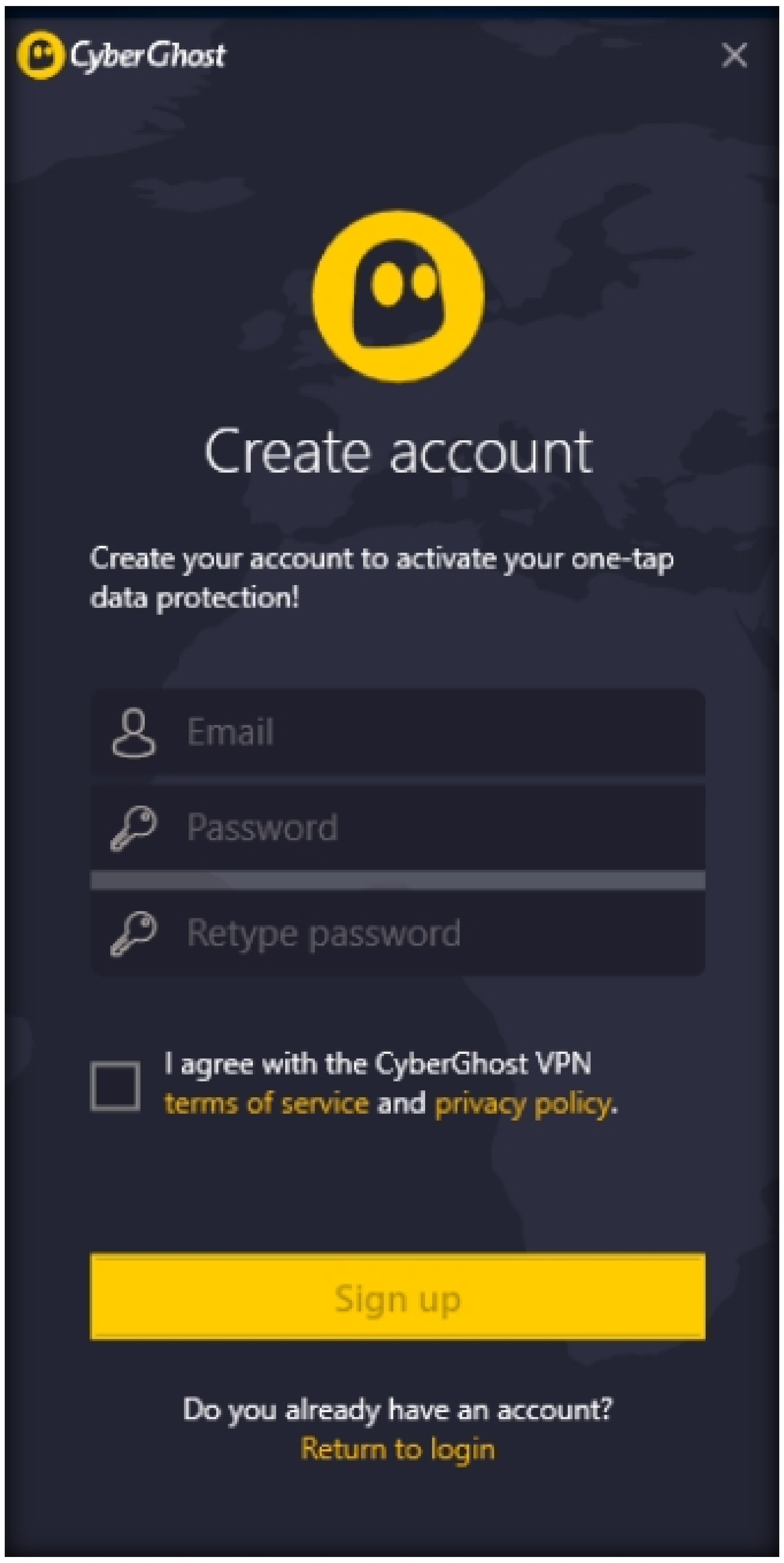
Name: TAP-Windows Provider V9 Network adapters
Publisher: OpenVPN Technologies, Inc.

☑ Always trust software from "OpenVPN Technologies, Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Figure 4.6.2: Windows Security pop-up

5. Once the installation is complete, the CyberGhost **Create account** window appears.



CyberGhost
Create account

Create your account to activate your one-tap data protection!

Email
Password
Retype password

☐ I agree with the CyberGhost VPN terms of service and privacy policy.

Sign up

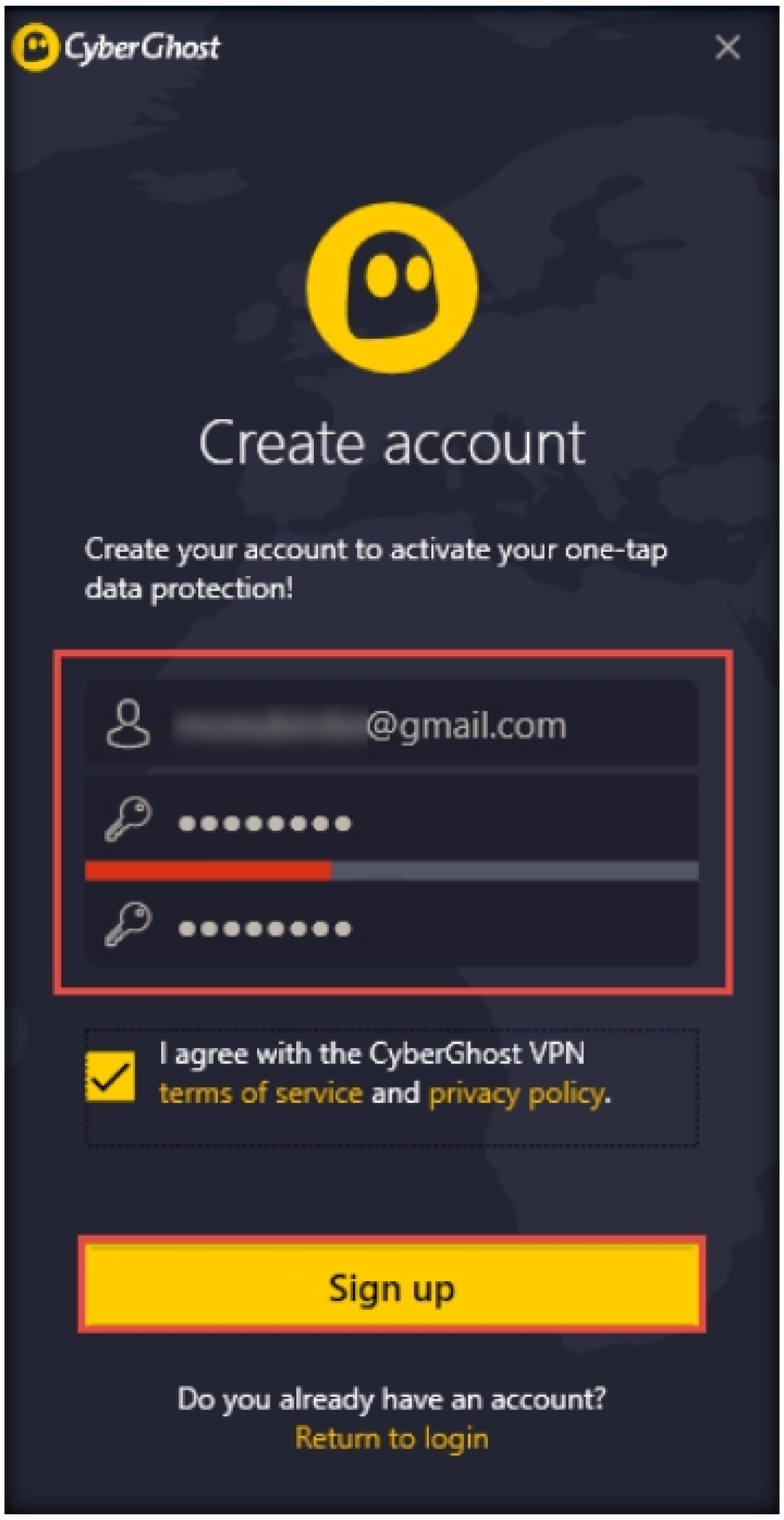
Do you already have an account?
Return to login

Figure 4.6.3: CyberGhost Create account window

TASK 6.2

Create Account

6. Create an account using your personal details and click on **Sign Up**.



Create your account to activate your one-tap data protection!

@gmail.com

••••••••

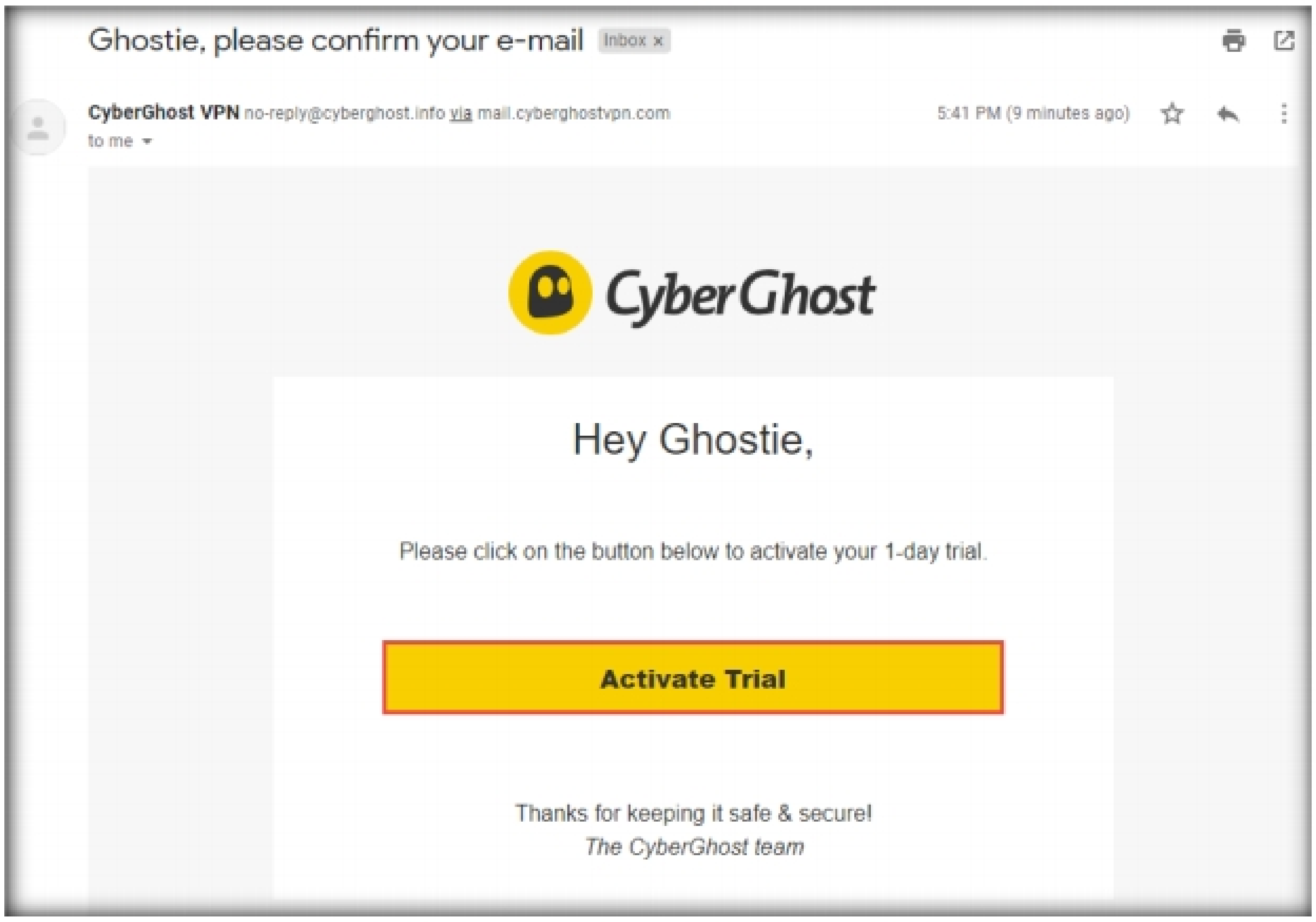
••••••••

☑ I agree with the CyberGhost VPN terms of service and privacy policy.

Do you already have an account?
Return to login

Figure 4.6.4: CyberGhost creating account

7. You will receive an activation email on your personal email. Open the email and click on **Activate Trial** to start your trial version of CyberGhost.



Ghostie, please confirm your e-mail

CyberGhost VPN no-reply@cyberghost.info via mail.cyberghostvpn.com
to me

5:41 PM (9 minutes ago)

Hey Ghostie,

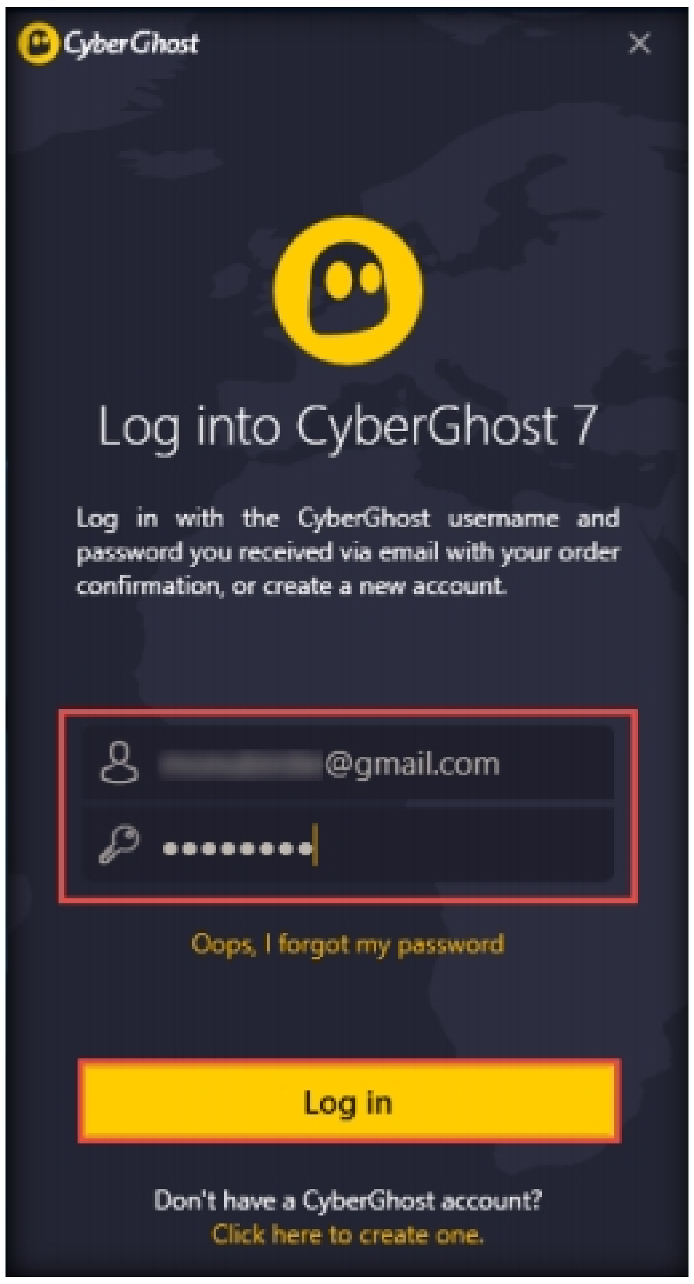
Please click on the button below to activate your 1-day trial.

Thanks for keeping it safe & secure!
The CyberGhost team

Inbox ×
CyberGhost
Activate Trial

Figure 4.6.5: Email for Activation of a trial version

8. Now, switch to the **CyberGhost** login page and log in with the email address and password provided earlier; click **Log in**.



Log into CyberGhost 7

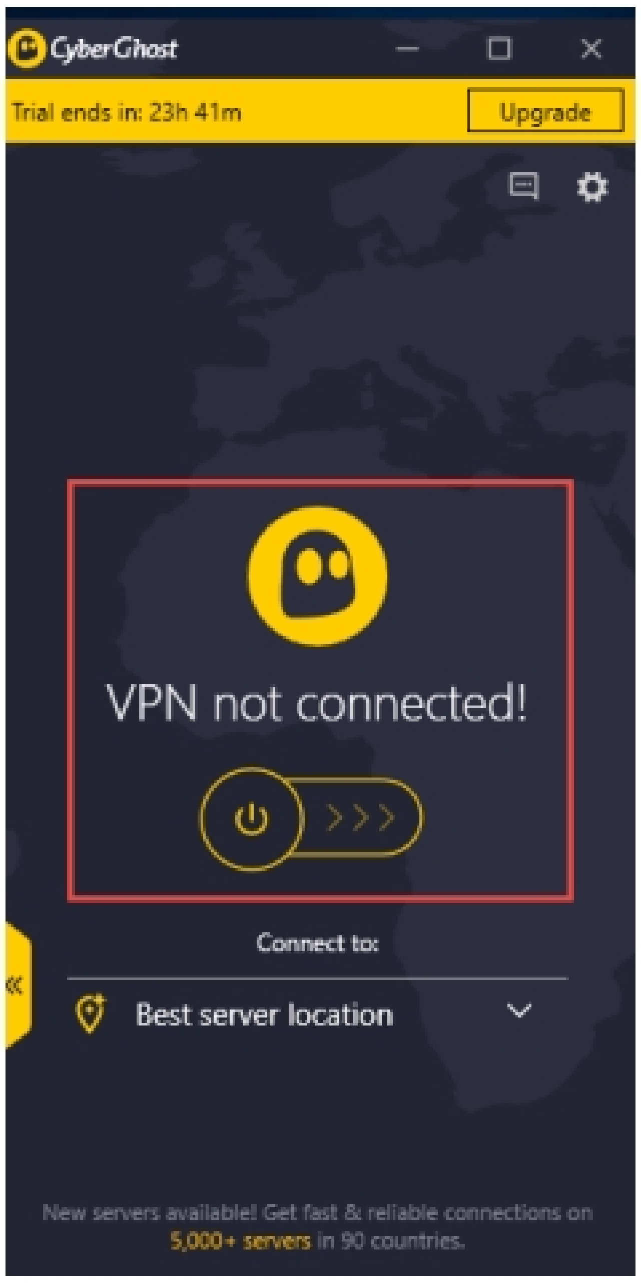
Log in with the CyberGhost username and password you received via email with your order confirmation, or create a new account.

[redacted]@gmail.com
••••••••

CyberGhost
Oops, I forgot my password
Log in
Don't have a CyberGhost account?
Click here to create one.

Figure 4.6.6: CyberGhost Log in

9. The CyberGhost window appears, displaying **VPN not connected!**


CyberGhost
Trial ends in: 23h 41m
Upgrade
VPN not connected!
Connect to:
Best server location

New servers available! Get fast & reliable connections on 5,000+ servers in 90 countries.

Figure 4.6.7: CyberGhost window

10. Now, click the **Settings** icon and select **Settings** from the options.

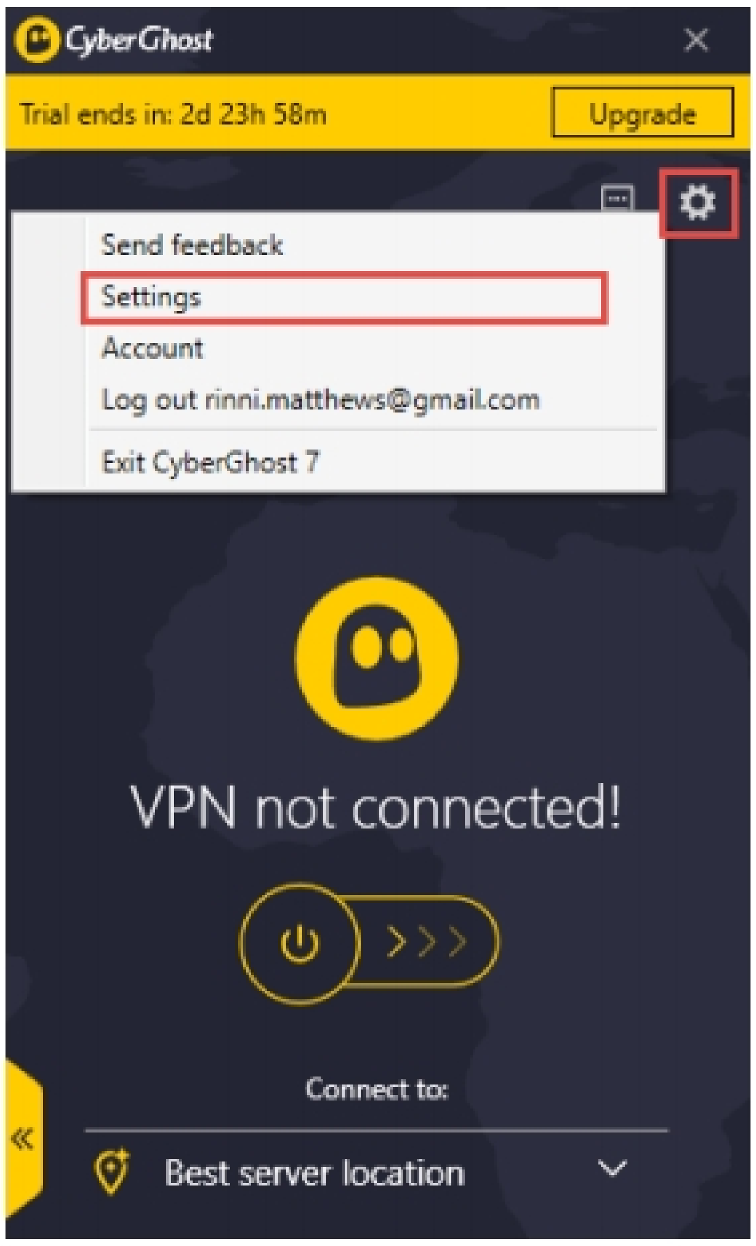

CyberGhost
Trial ends in: 2d 23h 58m
Upgrade
Send feedback
Settings
Account
Log out rinni.matthews@gmail.com
Exit CyberGhost 7
VPN not connected!
Connect to:
Best server location

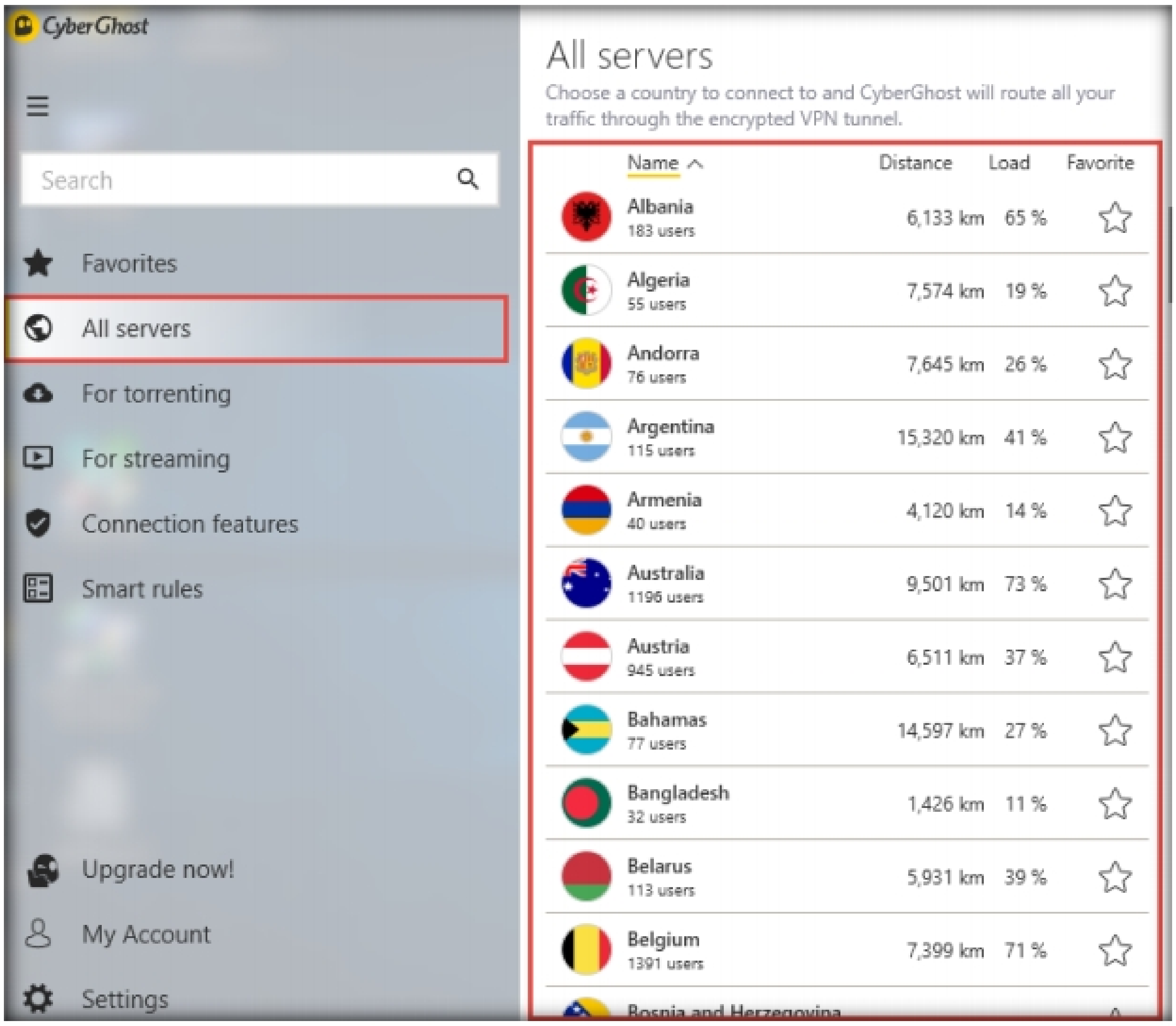
Figure 4.6.8: CyberGhost selecting the setting icon

TASK 6.3

Choose a Proxy from CyberGhost

11. The **CyberGhost Settings** window appears; click on **All server** from the left-hand pane.

Note: The list of the servers may vary in your lab environment


CyberGhost
☰
Search
Favorites
All servers
For torrenting
For streaming
Connection features
Smart rules
Upgrade now!
My Account
Settings

All servers

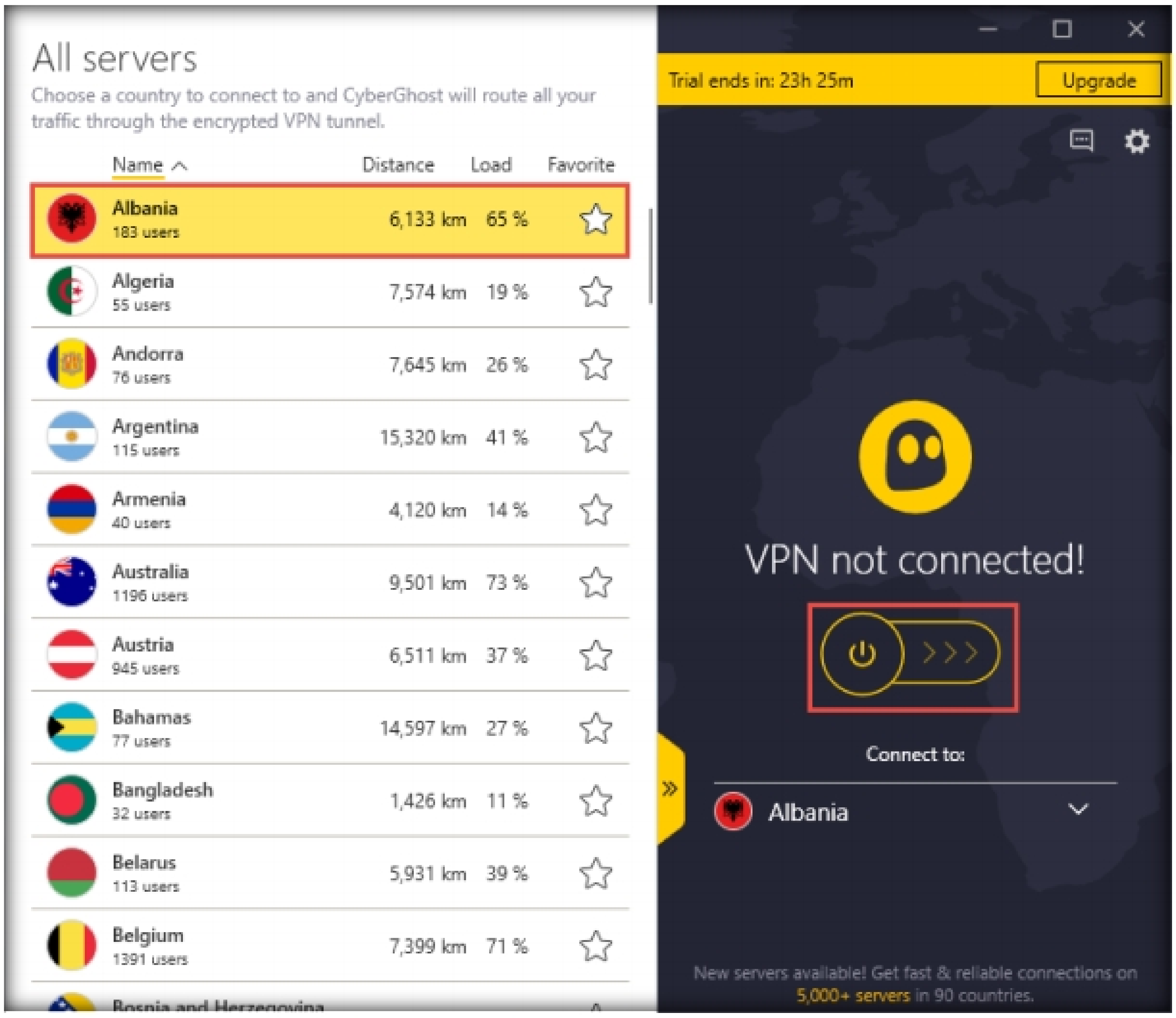
Choose a country to connect to and CyberGhost will route all your traffic through the encrypted VPN tunnel.

Name ^	Distance	Load	Favorite
Albania 183 users	6,133 km	65 %	☆
Algeria 55 users	7,574 km	19 %	☆
Andorra 76 users	7,645 km	26 %	☆
Argentina 115 users	15,320 km	41 %	☆
Armenia 40 users	4,120 km	14 %	☆
Australia 1196 users	9,501 km	73 %	☆
Austria 945 users	6,511 km	37 %	☆
Bahamas 77 users	14,597 km	27 %	☆
Bangladesh 32 users	1,426 km	11 %	☆
Belarus 113 users	5,931 km	39 %	☆
Belgium 1391 users	7,399 km	71 %	☆
Bosnia and Herzegovina			

Figure 4.6.9: CyberGhost All servers window

12. Click to select any proxy server from the available options in the **All servers** section (here, **Albania**) and click on the power icon (⏻) under **VPN now connected!**, as shown in the screenshot.

Note: If the CyberGhost window appears indicating that all free user slots are booked, then close the window and select another proxy server from the "all servers" list.



All servers

Choose a country to connect to and CyberGhost will route all your traffic through the encrypted VPN tunnel.

Name	Distance	Load	Favorite
Albania 183 users	6,133 km	65 %	☆
Algeria 55 users	7,574 km	19 %	☆
Andorra 76 users	7,645 km	26 %	☆
Argentina 115 users	15,320 km	41 %	☆
Armenia 40 users	4,120 km	14 %	☆
Australia 1196 users	9,501 km	73 %	☆
Austria 945 users	6,511 km	37 %	☆
Bahamas 77 users	14,597 km	27 %	☆
Bangladesh 32 users	1,426 km	11 %	☆
Belarus 113 users	5,931 km	39 %	☆
Belgium 1391 users	7,399 km	71 %	☆
Bosnia and Herzegovina			

Trial ends in: 23h 25m

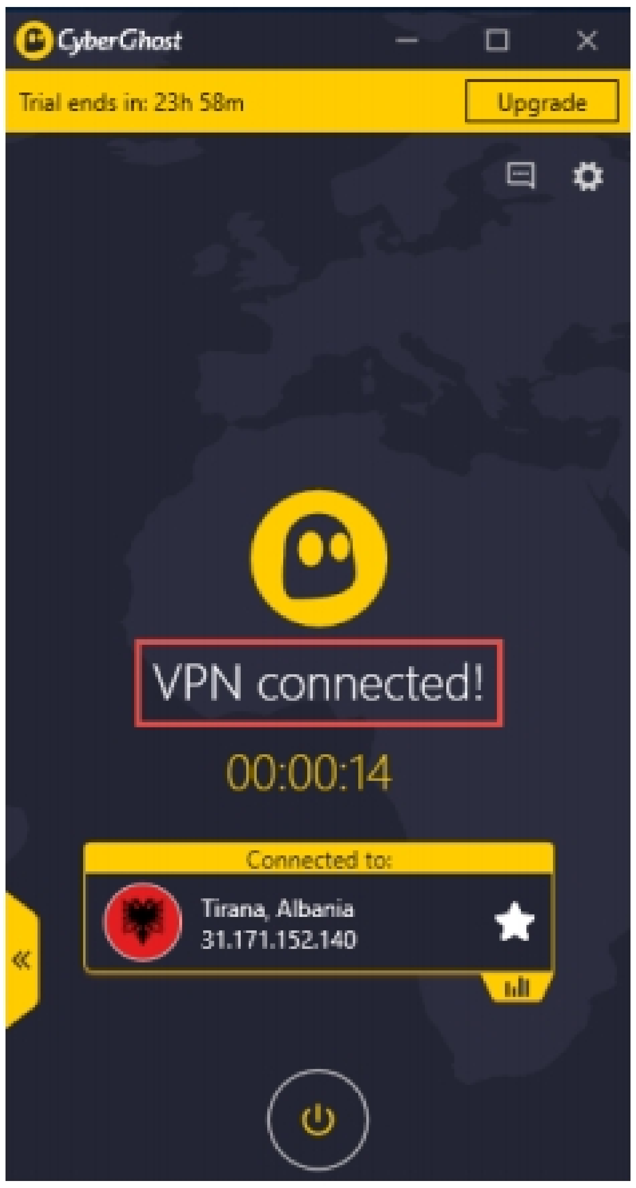
VPN not connected!

Connect to: Albania

New servers available! Get fast & reliable connections on 5,000+ servers in 90 countries.

Figure 4.6.10: CyberGhost selecting proxy server

13. **CyberGhost** attempts to establish a connection to the proxy server. On successfully establishing a connection, **VPN connected!** appears.



Trial ends in: 23h 58m

VPN connected!

00:00:14

Connected to:
Tirana, Albania
31.171.152.140

Figure 4.6.11: CyberGhost connection established

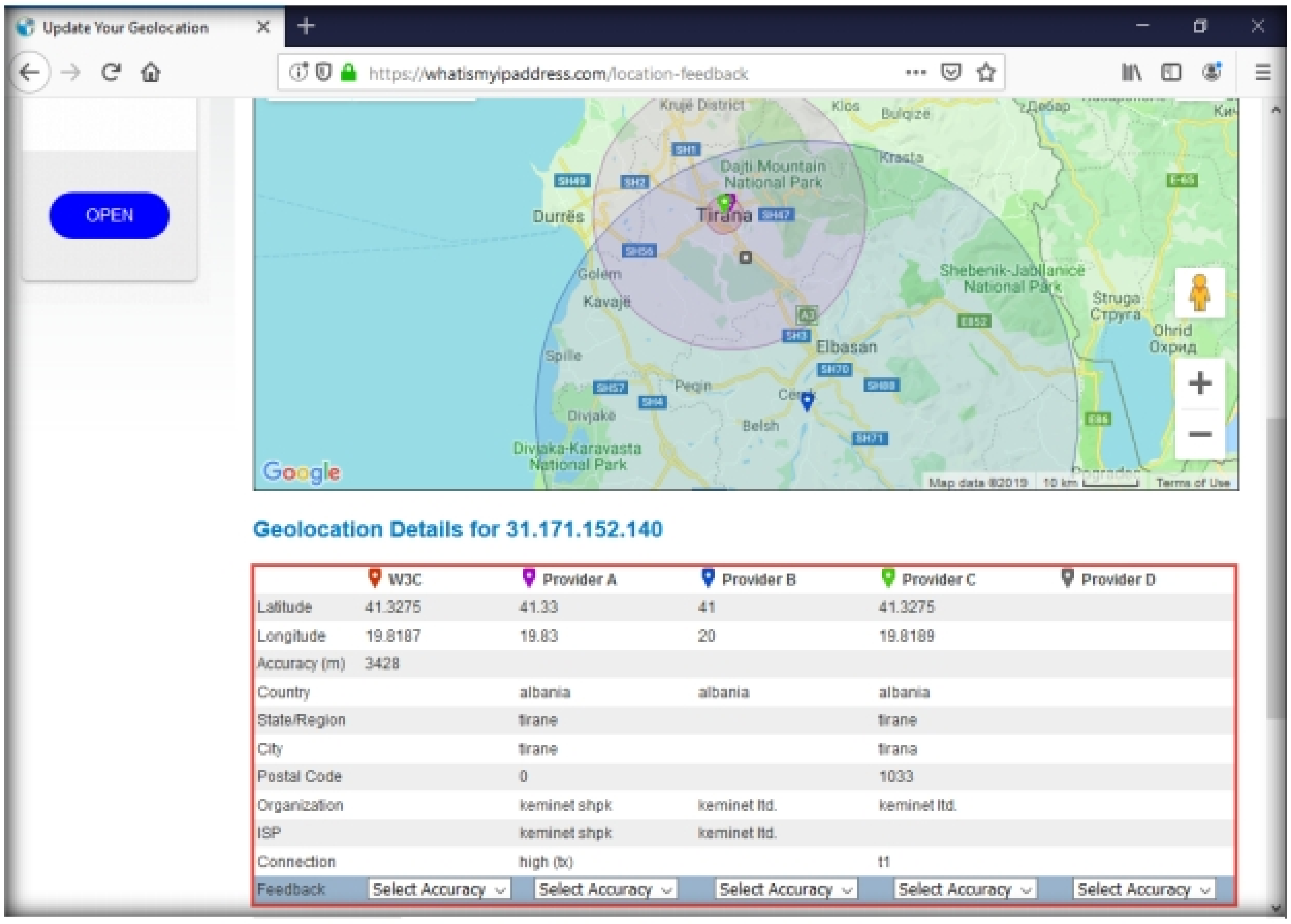
TASK 6.4

Browse Internet

14. Minimize the **CyberGhost** window and launch the **Mozilla Firefox** web browser; type the URL **https://whatismyipaddress.com/location-feedback** in the address bar and press **Enter**.

Note: If a **Will you allow whatismyipaddress.com to access your location?** pop-up appears, click **Allow Location Access**.

15. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **31.171.152.140** and **Albania**.


Update Your Geolocation
https://whatismyipaddress.com/location-feedback
OPEN
Tirana
Durrës
Elbasan
Google
Map data ©2019 10 km Terms of Use

Geolocation Details for 31.171.152.140

	W3C	Provider A	Provider B	Provider C	Provider D
Latitude	41.3275	41.33	41	41.3275	
Longitude	19.8187	19.83	20	19.8189	
Accuracy (m)	3428				
Country		albania	albania	albania	
State/Region		tirane		tirane	
City		tirane		tirana	
Postal Code		0		1033	
Organization		keminet shpk	keminet ltd.	keminet ltd.	
ISP		keminet shpk	keminet ltd.		
Connection		high (tx)		t1	
Feedback	Select Accuracy	Select Accuracy	Select Accuracy	Select Accuracy	Select Accuracy

Figure 4.6.12: Testing your IP address

16. Open a new tab in the **web browser** and surf anonymously using this proxy.

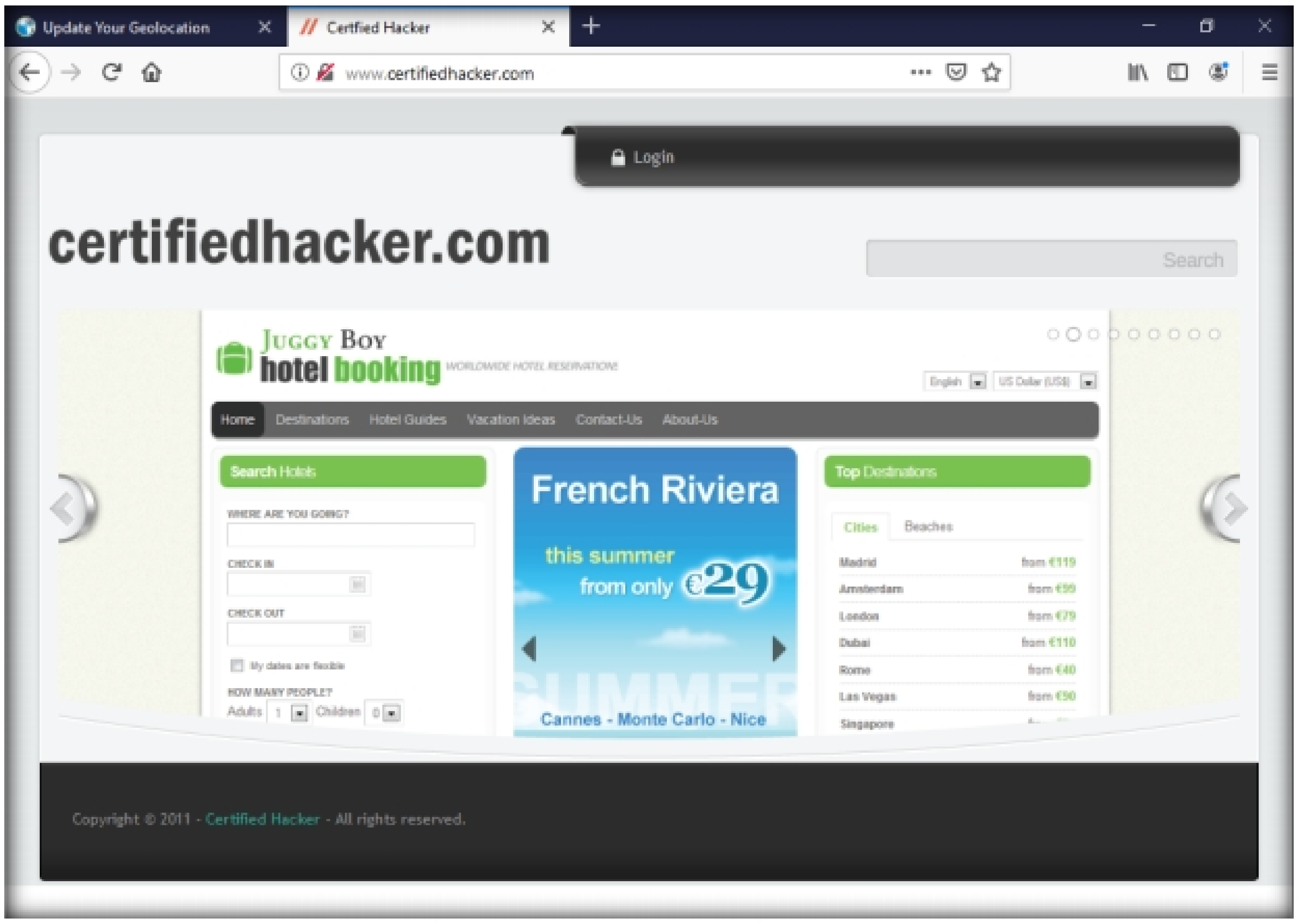

Update Your Geolocation
Certfied Hacker
www.certifiedhacker.com
Login
certifiedhacker.com
Search
Juggy Boy hotel booking
Home Destinations Hotel Guides Vacation Ideas Contact-Us About-Us
Search Hotels
French Riviera
this summer from only €29
Cannes - Monte Carlo - Nice
Top Destinations
Copyright © 2011 - Certified Hacker - All rights reserved.

Figure 4.6.13: Surfing internet using Proxy server

17. Once you are done browsing, in the CyberGhost window, click the **Power** icon to disconnect the proxy, as shown in the screenshot.

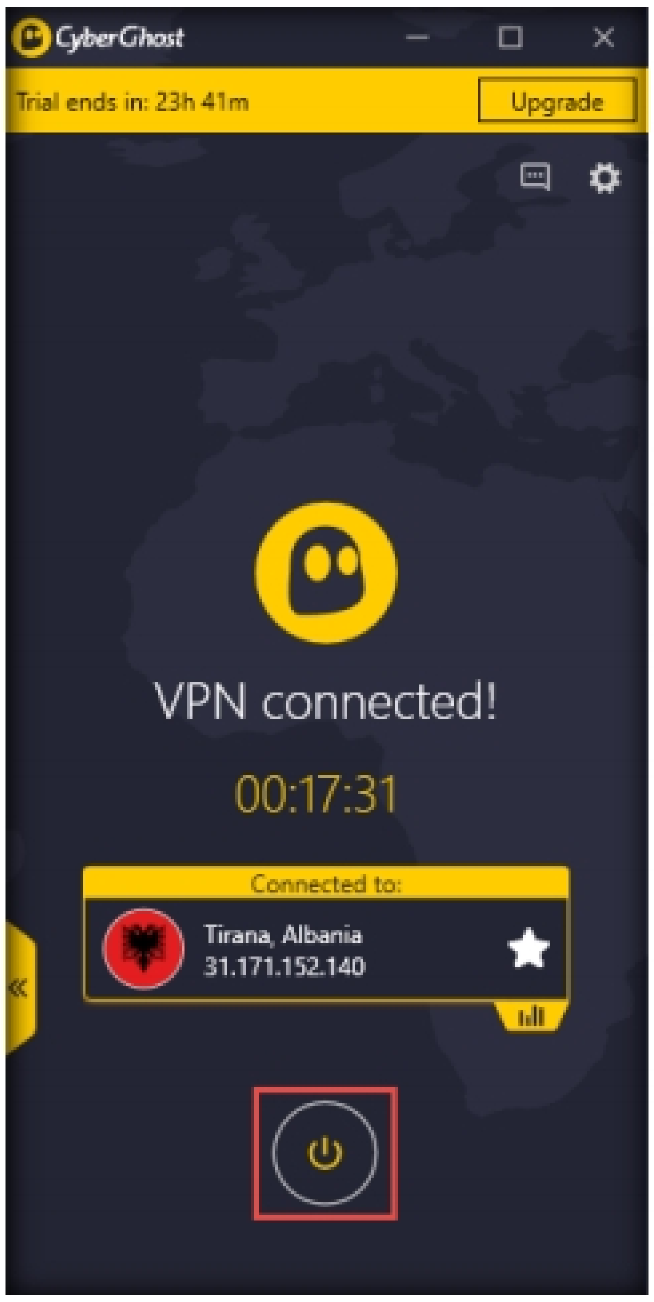

CyberGhost
Trial ends in: 23h 41m
Upgrade
VPN connected!
00:17:31
Connected to:
Tirana, Albania
31.171.152.140

Figure 4.6.14: Turning Off the Proxy

18. This concludes the demonstration of anonymously surfing the Internet using CyberGhost.
19. Close all open windows and document all the acquired information.
20. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall the **CyberGhost VPN** application
21. Turn off the **Windows 10** virtual machine.

You can also use other proxy tools such as **Burp Suite** (https://www.portswigger.net), **Tor** (https://www.torproject.org), **CCProxy** (https://www.youngzsoft.net), and **Hotspot Shield** (https://www.hotspotshield.com) to browse the Internet anonymously.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Draw Network Diagrams

A network diagram helps to analyze complete network topology.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Until now, you have gathered information about the open ports, services running on the ports, OS details, security mechanisms details, etc. of the target network using various port and network scanning techniques and tools.

As a professional ethical hacker or a pen tester, the last step in the penetration process is to draw a network diagram that assists in identifying the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables you to understand the position of firewalls, IDSs, routers, and other access control devices.

As a professional ethical hacker or pen tester, you should be able to create a pictorial representation of network topology used in the target network. The network diagrams can be used to launch further attacks on the target network.

Lab Objectives

- Draw network diagrams using Network Topology Mapper

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Network Topology Mapper located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**
- You can also download the latest version of the above-mentioned tool from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 10 Minutes

Overview of Network Diagrams

Drawing a network diagram assists in the identification of the topology or architecture of a target network, and further assists you in finding the vulnerabilities or weak points of security mechanisms. These vulnerabilities can then be exploited to bypass the target's network. The network diagram also helps the network administrators to manage their networks.

Lab Tasks

TASK 1

Draw Network Diagrams using Network Topology Mapper

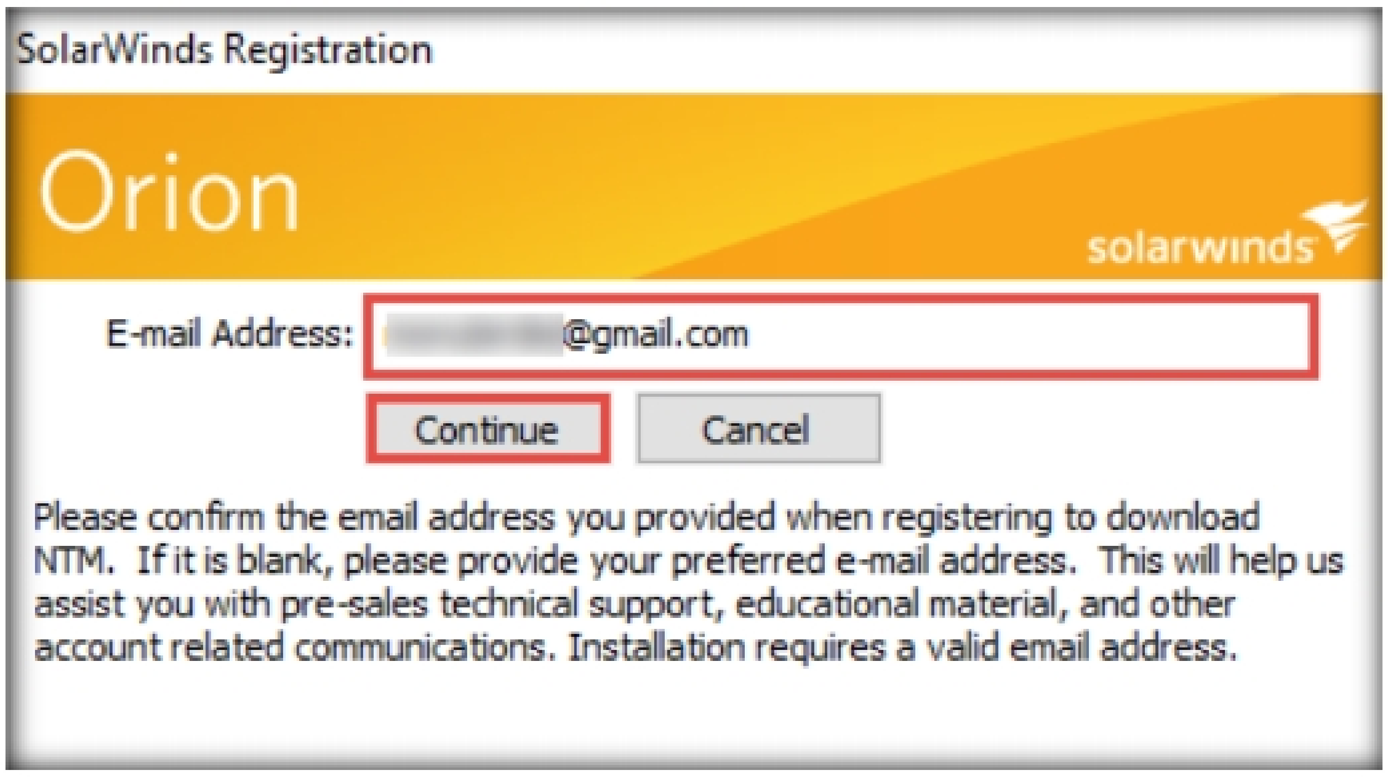
Here, we will use Network Topology Mapper to draw network diagrams of the target network.

TASK 1.1

Install Network Topology Mapper

1. Turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, and then double-click **SolarWinds Network Topology Mapper.exe**.
3. The **SolarWinds Registration** dialog-box opens. Enter a working email address, and then click **Continue**.

Network Topology Mapper discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data. It automatically detects new devices and changes to network topology, simplifies inventory management for hardware and software assets, and addresses reporting needs for PCI compliance and other regulatory requirements.



E-mail Address: [redacted]@gmail.com

Please confirm the email address you provided when registering to download NTM. If it is blank, please provide your preferred e-mail address. This will help us assist you with pre-sales technical support, educational material, and other account related communications. Installation requires a valid email address.

Figure 5.1.1: SolarWinds Registration dialog-box

4. In the next window, accept the license agreement and click **Install**.

Note: If a **User Account Control** window appears, click **Yes**.

5. The SolarWinds license pop-up appears; click **Continue Evaluation**.

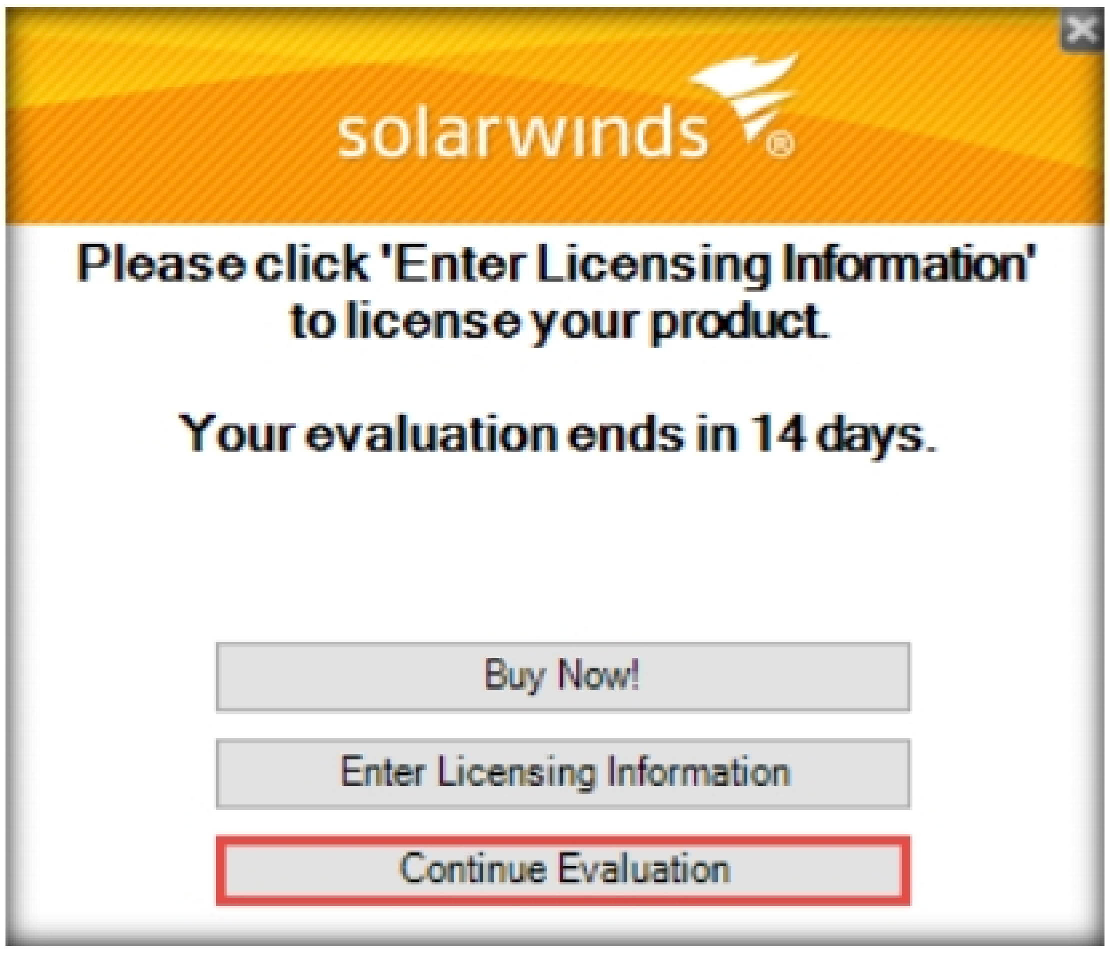
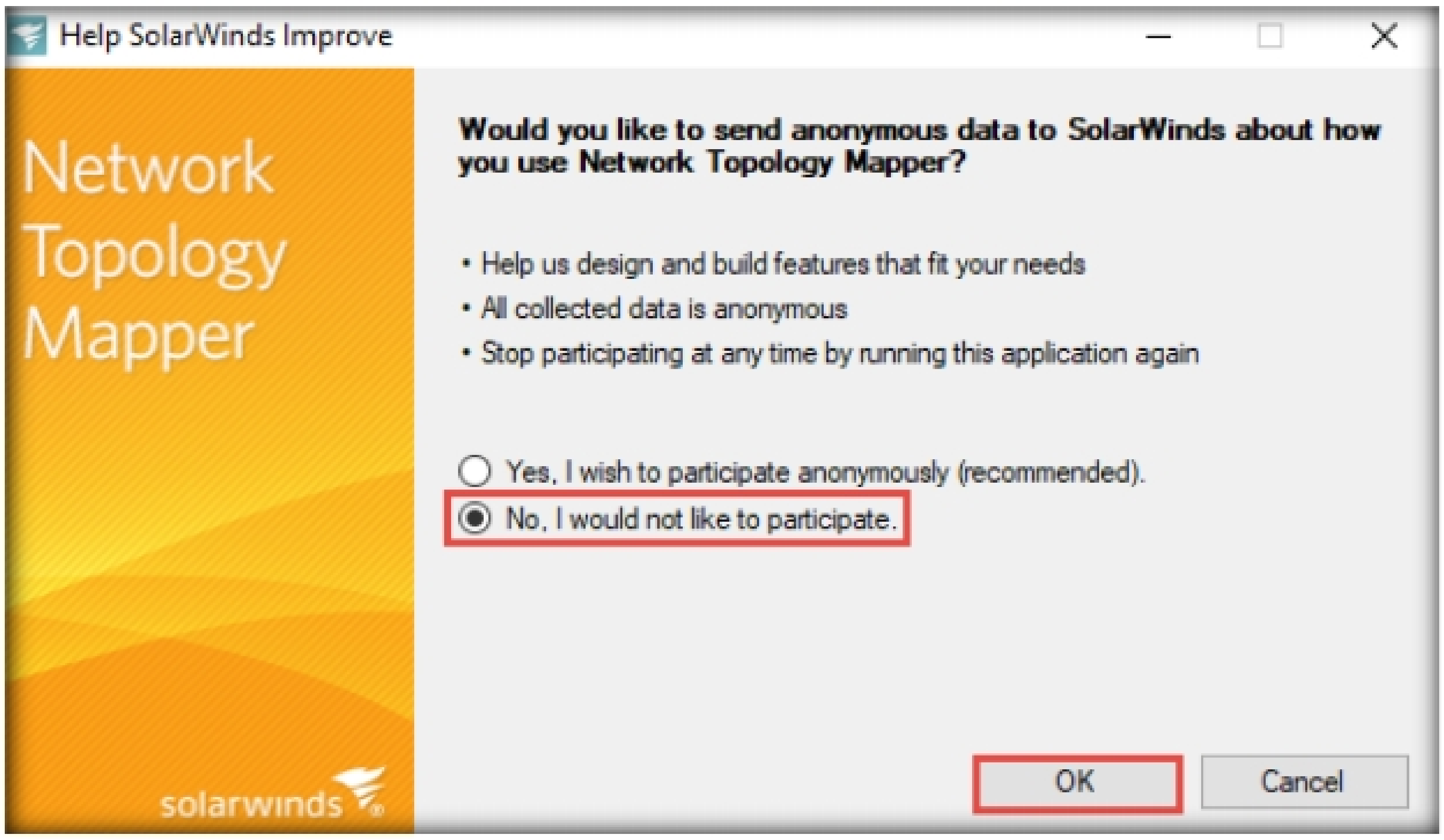

solarwinds
Please click 'Enter Licensing Information' to license your product.
Your evaluation ends in 14 days.
Buy Now!
Enter Licensing Information
Continue Evaluation

Figure 5.1.2: Solarwinds license pop-up

6. The **Help SolarWinds Improve** window appears. Click the **No, I would not like to participate** radio button, and then click **OK**.


Help SolarWinds Improve
Network Topology Mapper
solarwinds
OK
Cancel

Would you like to send anonymous data to SolarWinds about how you use Network Topology Mapper?

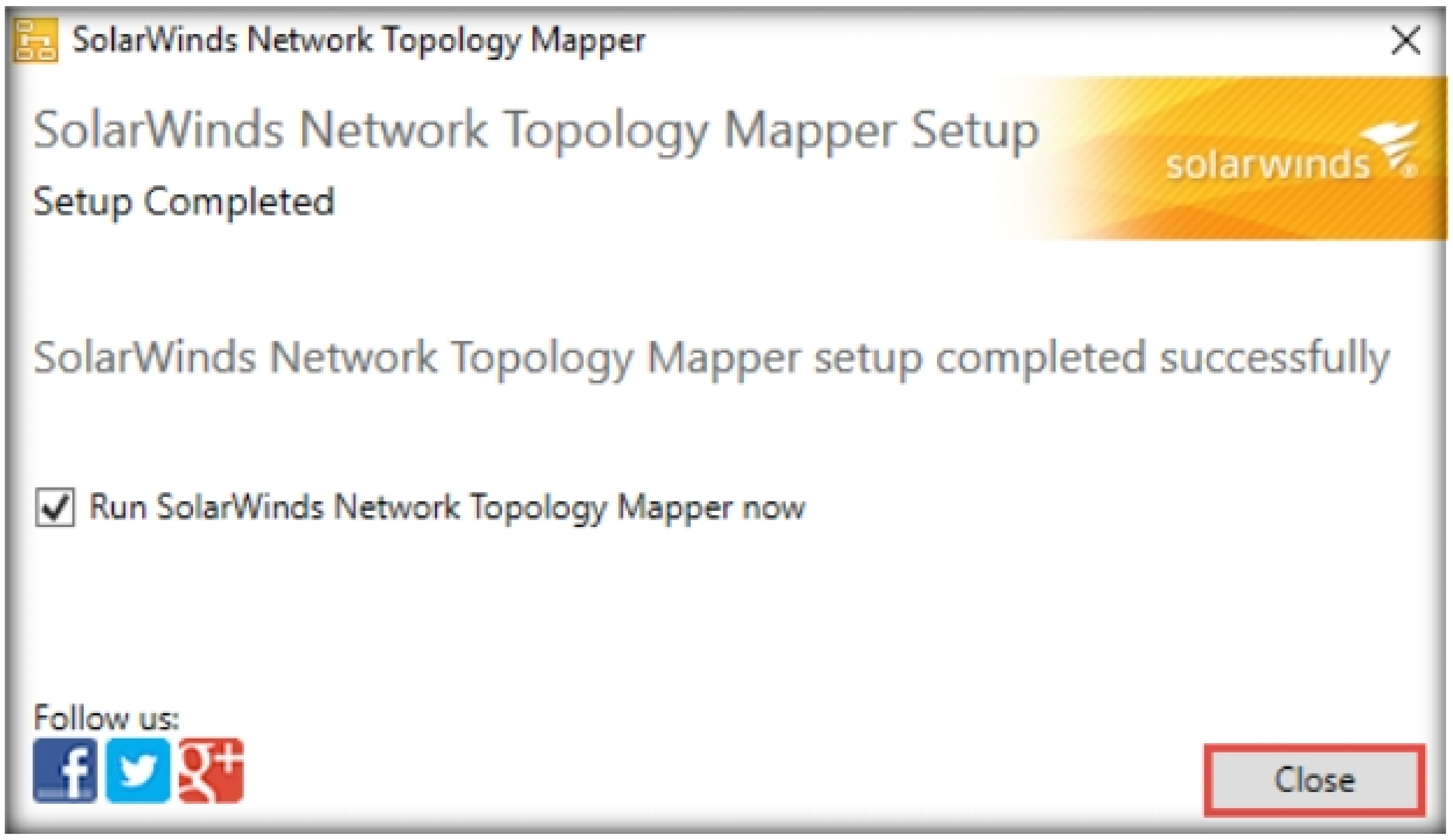
- Help us design and build features that fit your needs
- All collected data is anonymous
- Stop participating at any time by running this application again

○ Yes, I wish to participate anonymously (recommended).
● No, I would not like to participate.

Figure 5.1.3: Help SolarWinds Improve window

7. Once the installation is complete, and the **SolarWinds Network Topology Mapper** window opens, click **Close**.

Note: Ensure that the **Run SolarWinds Network Topology Mapper now** option is selected.



SolarWinds Network Topology Mapper

SolarWinds Network Topology Mapper Setup

Setup Completed

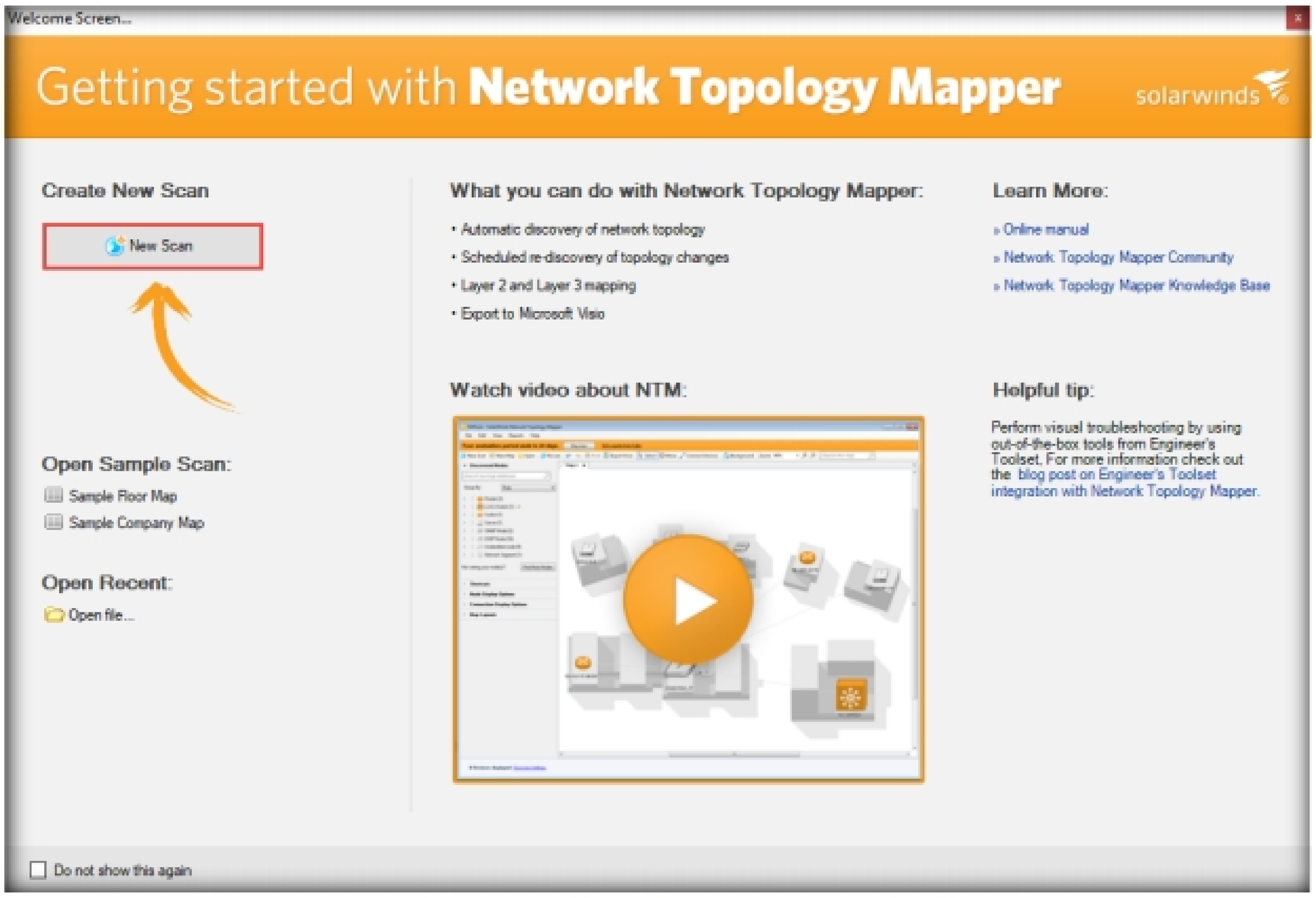
SolarWinds Network Topology Mapper setup completed successfully

☑ Run SolarWinds Network Topology Mapper now

Figure 5.1.4: SolarWinds setup completed window

8. The **Solarwinds** pop-up opens; click **Continue Evaluation**.

9. The **SolarWinds Network Topology Mapper** main window appears, along with the **Welcome Screen…**. Click **New Scan** in the left-hand pane of the **Welcome Screen**.



Welcome Screen...

Getting started with **Network Topology Mapper**

Create New Scan

What you can do with Network Topology Mapper:

- Automatic discovery of network topology
- Scheduled re-discovery of topology changes
- Layer 2 and Layer 3 mapping
- Export to Microsoft Visio

Learn More:

» Online manual
» Network Topology Mapper Community
» Network Topology Mapper Knowledge Base

Watch video about NTM:

Helpful tip:

Perform visual troubleshooting by using out-of-the-box tools from Engineer's Toolset. For more information check out the blog post on Engineer's Toolset integration with Network Topology Mapper.

Open Sample Scan:

Sample Floor Map
Sample Company Map

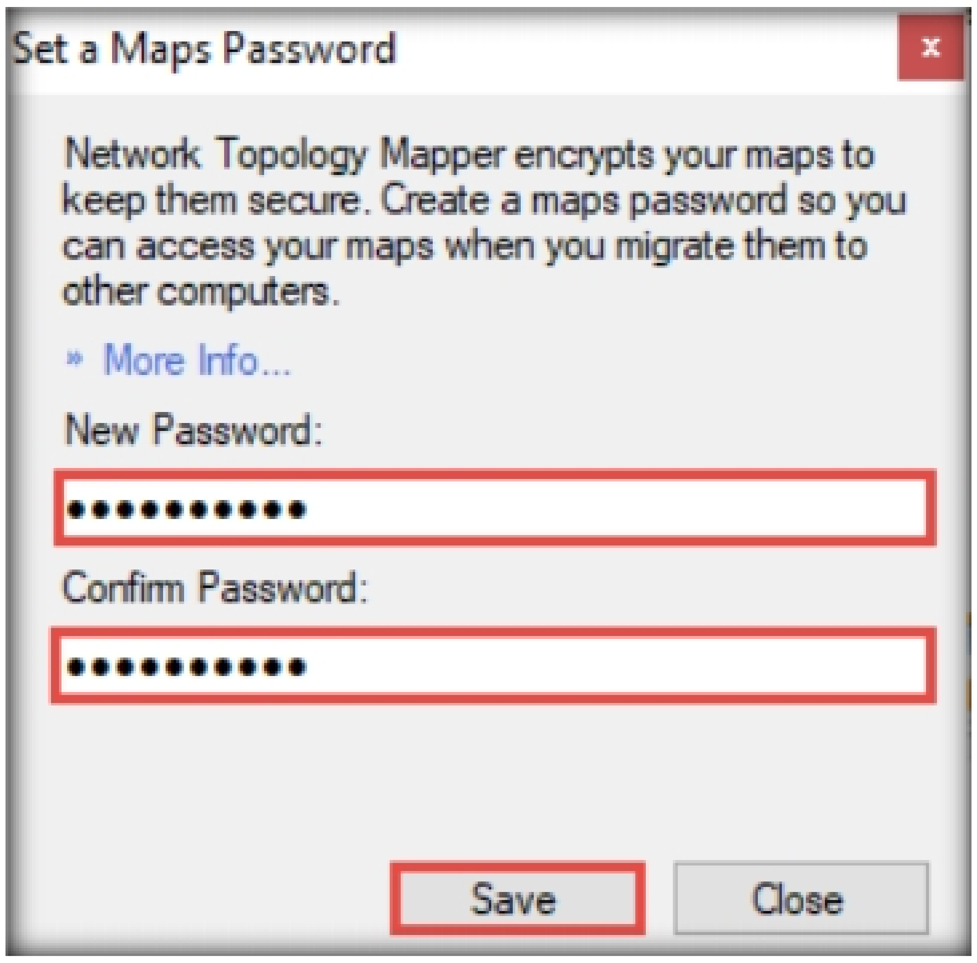
Open Recent:

Open file...

☐ Do not show this again

Figure 5.1.5: SolarWinds Network Topology Mapper main window

10. The **Set a Maps Password** pop-up appears. Enter a password (here **qwerty@123**) of your choice in the **New Password** field, re-enter the same password in the **Confirm Password** field, and click **Save**.



Set a Maps Password

Network Topology Mapper encrypts your maps to keep them secure. Create a maps password so you can access your maps when you migrate them to other computers.

» More Info...

New Password: ••••••••••

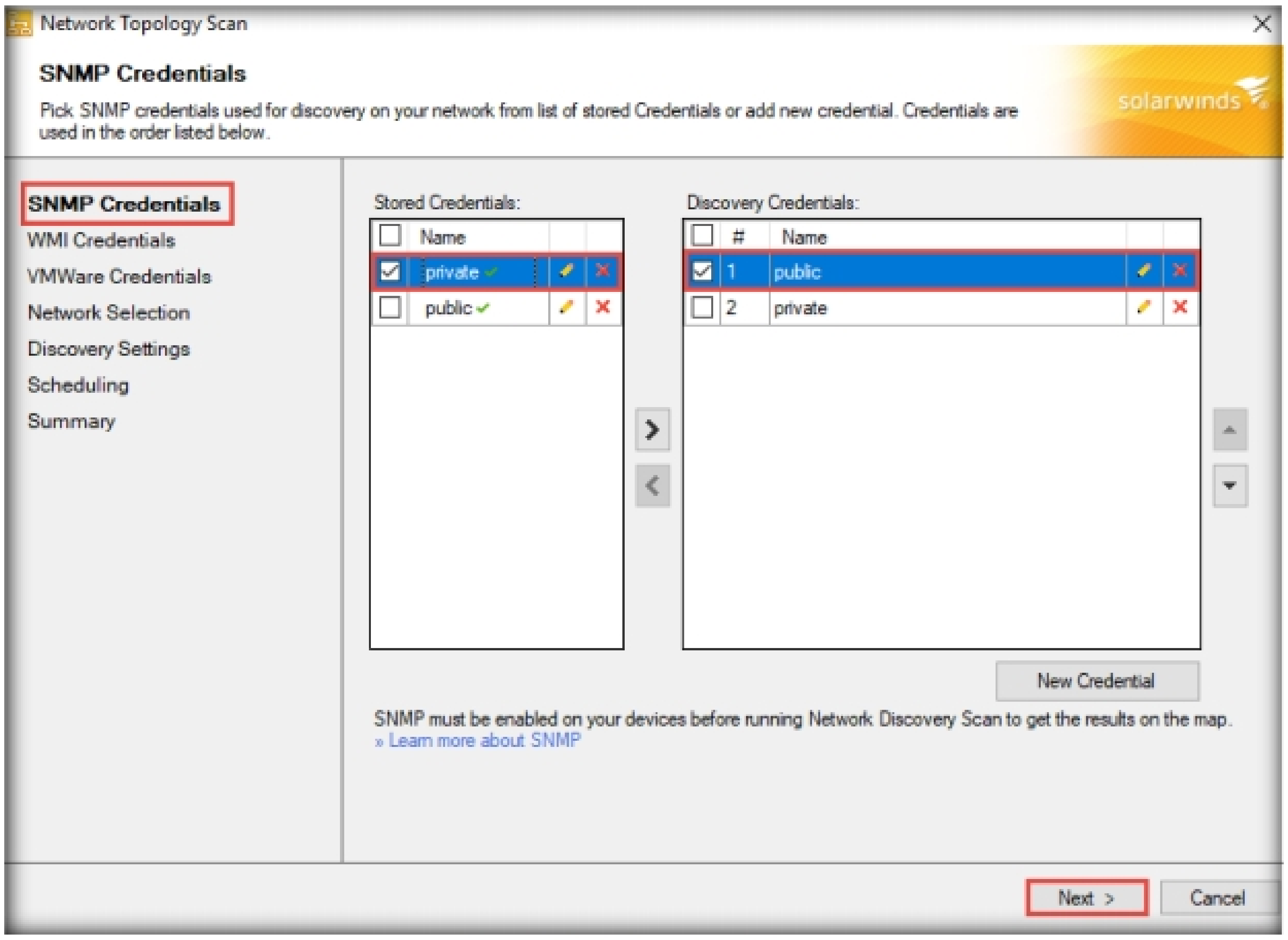
Confirm Password: ••••••••••

Figure 5.1.6: Set a Maps Password window

TASK 1.2

Configure Network Topology Mapper

11. The **Network Topology Scan** window appears. In the **SNMP Credentials** section, select the **private** credential under the **Stored Credentials** section and **public** credential under the **Discovery Credentials** section, and then click **Next**.



Network Topology Scan

SNMP Credentials

Pick SNMP credentials used for discovery on your network from list of stored Credentials or add new credential. Credentials are used in the order listed below.

solarwinds
SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary

Stored Credentials:

☐	Name
☑	private ✓
☐	public ✓

Discovery Credentials:

☐	#	Name
☑	1	public
☐	2	private

New Credential

SNMP must be enabled on your devices before running Network Discovery Scan to get the results on the map.

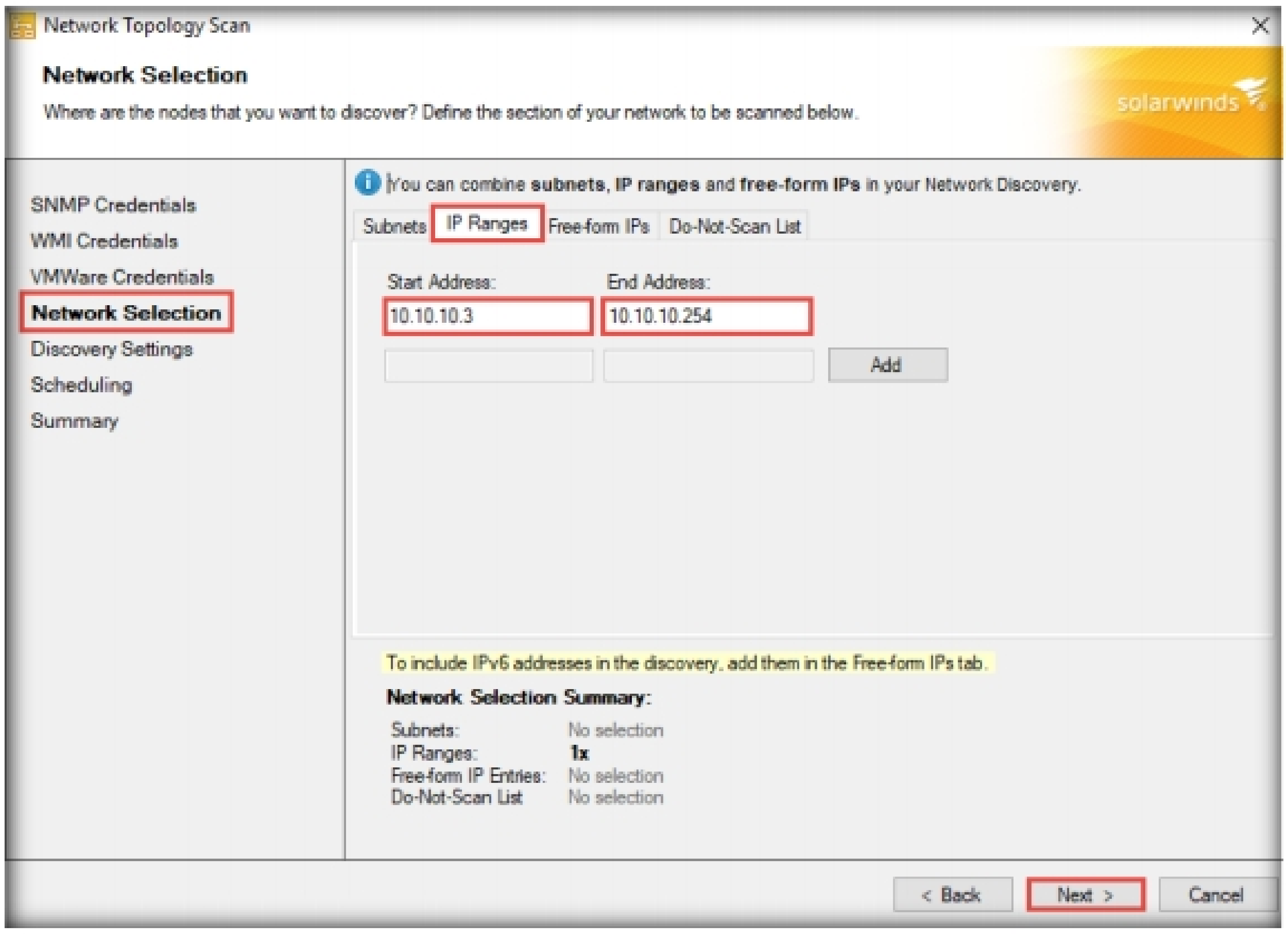
» Learn more about SNMP

Next >
Cancel

Figure 5.1.7: SNMP Credentials section

12. Leave the **WMI Credentials** and **VMWare Credentials** section to default and click **Next**.

13. The **Network Selection** section appears. Click the **IP Ranges** tab in the right-pane, enter the IP address range (**10.10.10.3 - 10.10.10.254**) in the **Start Address** and **End Address** fields, and click **Next**.



Network Topology Scan

Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

You can combine **subnets**, **IP ranges** and **free-form IPs** in your Network Discovery.

Start Address: 10.10.10.3

End Address: 10.10.10.254

To include IPv6 addresses in the discovery, add them in the Free-form IPs tab.

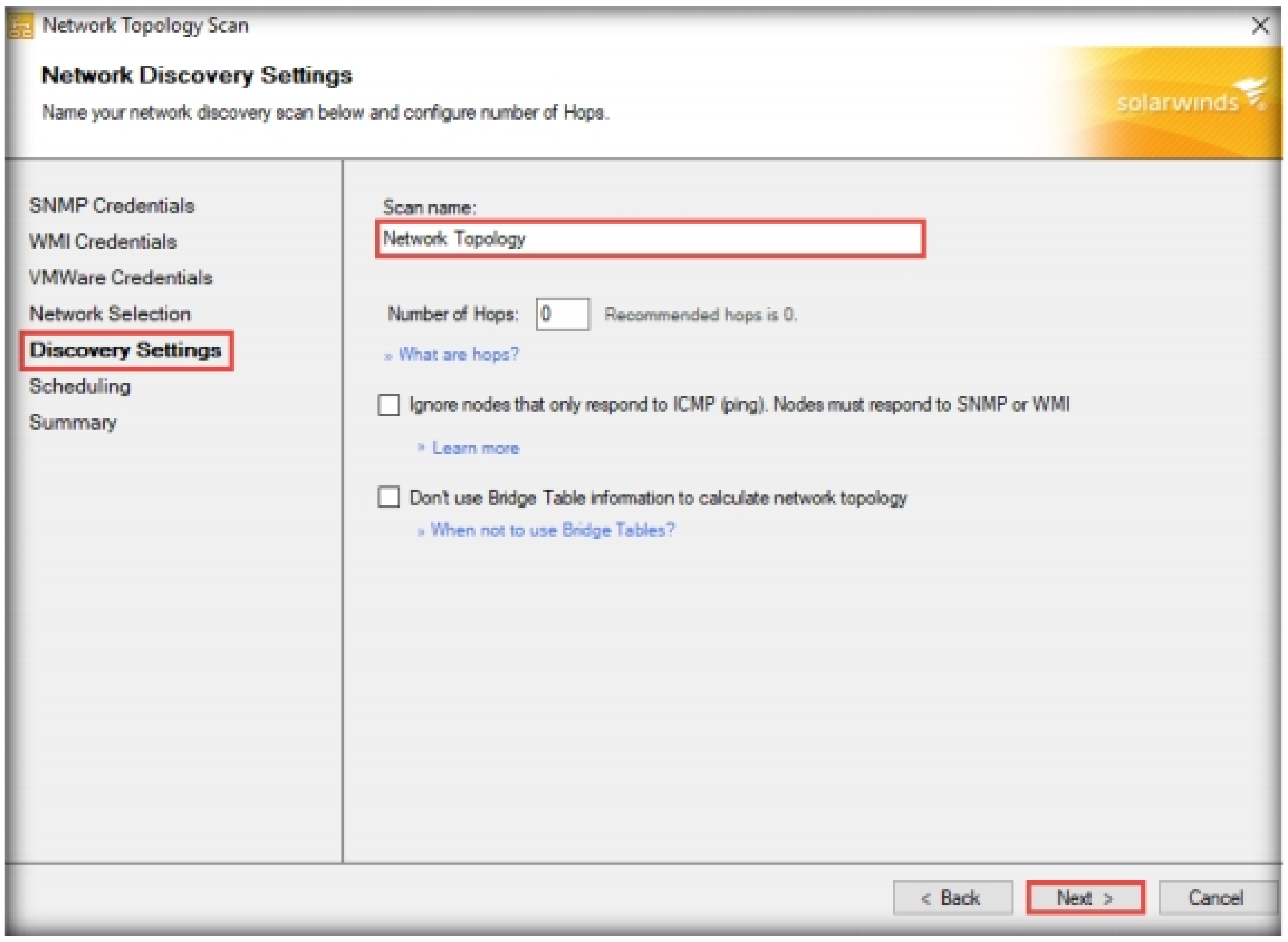
Network Selection Summary:

Subnets: No selection
IP Ranges: 1x
Free-form IP Entries: No selection
Do-Not-Scan List No selection

solarwinds
SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary
Subnets
IP Ranges
Free-form IPs
Do-Not-Scan List
Add
< Back
Next >
Cancel

Figure 5.1.8: Network Selection section

14. The **Discovery Settings** section appears. Enter a name under the **Scan name** field (here, "**Network Topology**") and click **Next**.



Network Topology Scan

Network Discovery Settings

Name your network discovery scan below and configure number of Hops.

Scan name: Network Topology

Number of Hops: 0 Recommended hops is 0.

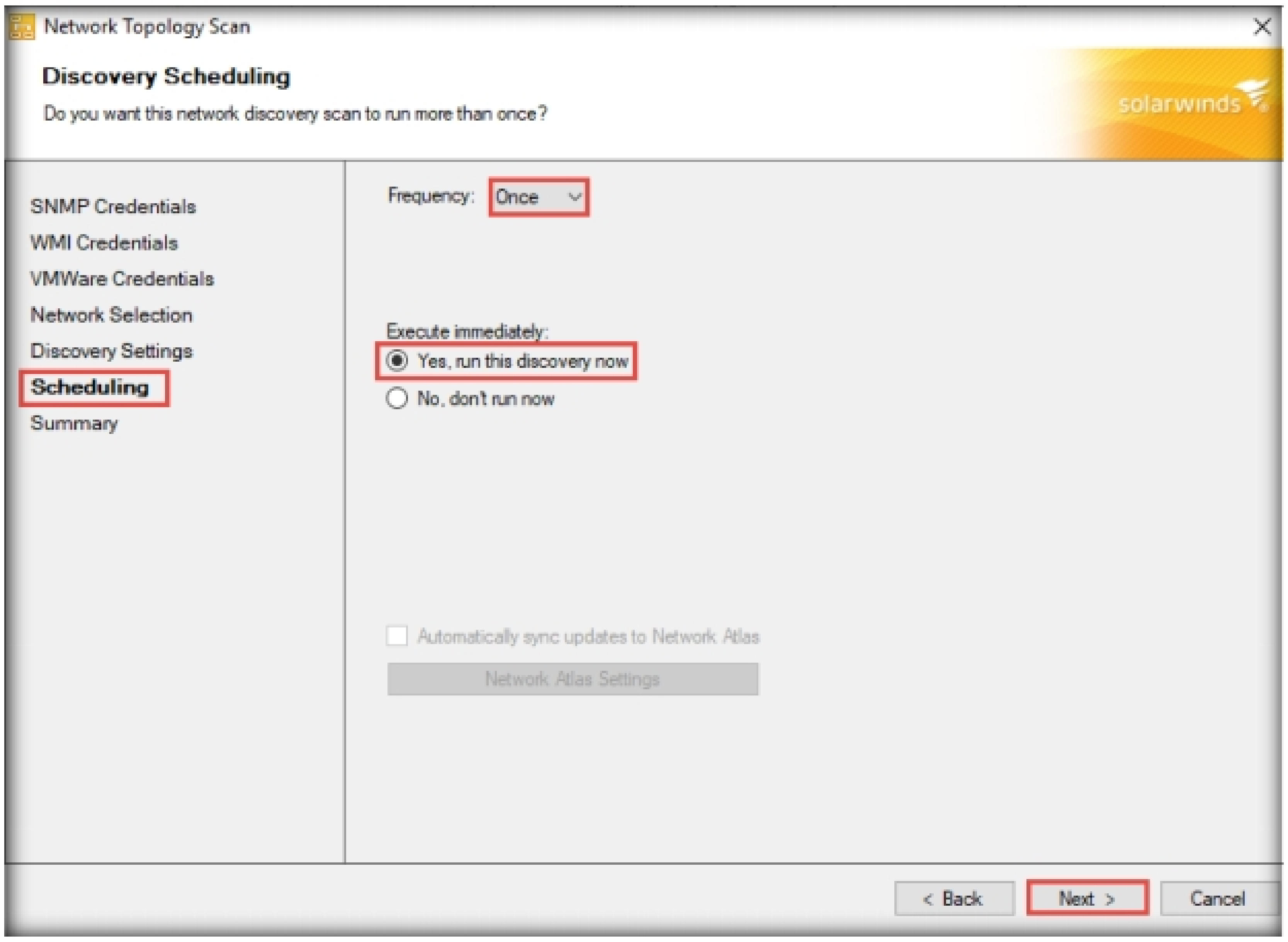
☐ Ignore nodes that only respond to ICMP (ping). Nodes must respond to SNMP or WMI

☐ Don't use Bridge Table information to calculate network topology

solarwinds
SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary
» What are hops?
» Learn more
» When not to use Bridge Tables?
< Back
Next >
Cancel

Figure 5.1.9: Discovery Settings section

15. The **Scheduling** section appears. Ensure that **Once** is selected in the **Frequency** drop-down menu; under the **Execute immediately** radio button **Yes, run this discovery now** is selected; then, click **Next**.



Network Topology Scan

Discovery Scheduling

Do you want this network discovery scan to run more than once?

Frequency: Once

Execute immediately:

● Yes, run this discovery now

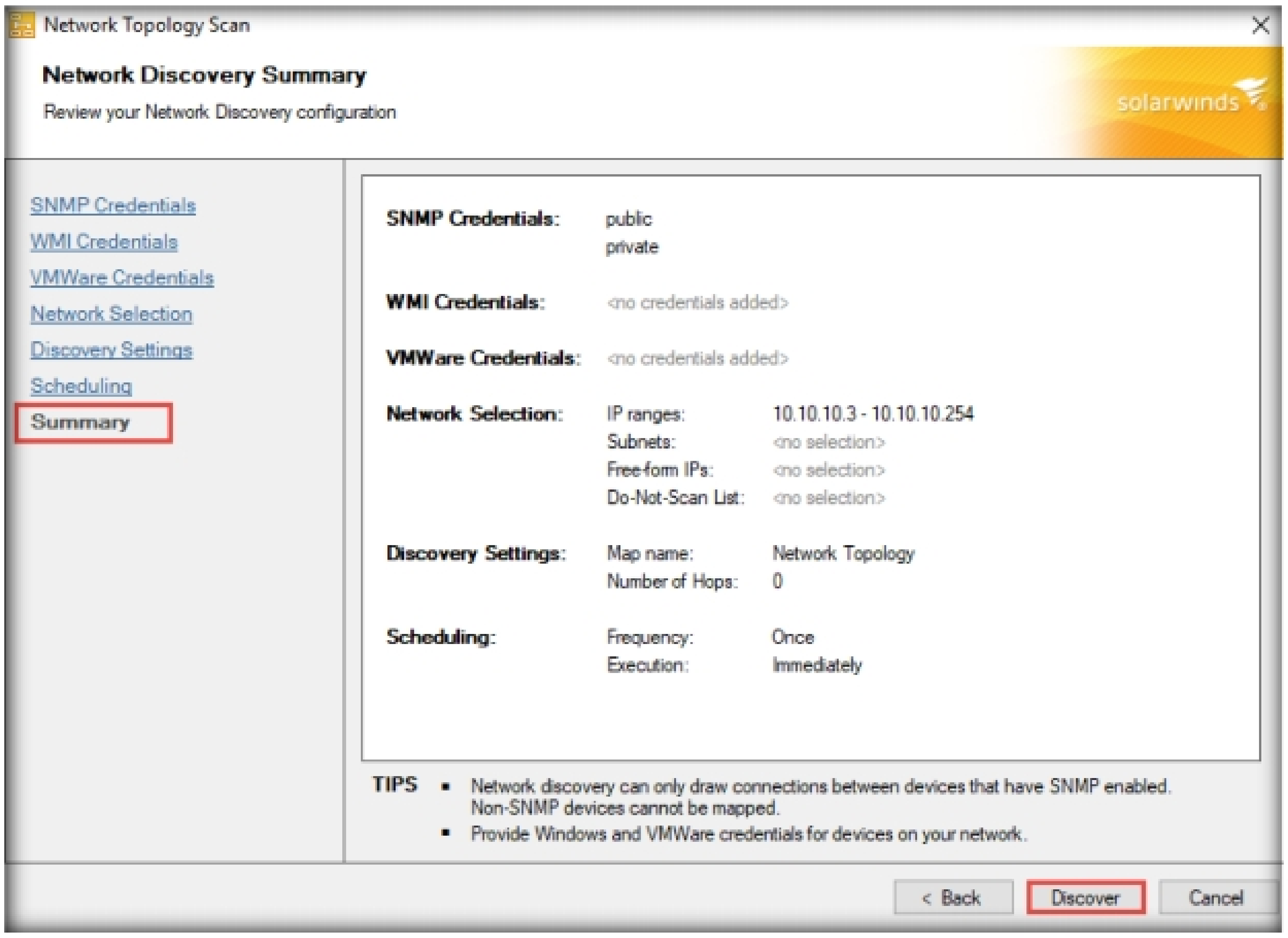
○ No, don't run now

☐ Automatically sync updates to Network Atlas

solarwinds
SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary
Network Atlas Settings
< Back
Next >
Cancel

Figure 5.1.10: Scheduling section

16. The **Summary** section appears; click **Discover**.



Network Topology Scan

Network Discovery Summary

Review your Network Discovery configuration

SNMP Credentials: public
private

WMI Credentials: <no credentials added>

VMWare Credentials: <no credentials added>

Network Selection:
IP ranges: 10.10.10.3 - 10.10.10.254
Subnets: <no selection>
Free-form IPs: <no selection>
Do-Not-Scan List: <no selection>

Discovery Settings:
Map name: Network Topology
Number of Hops: 0

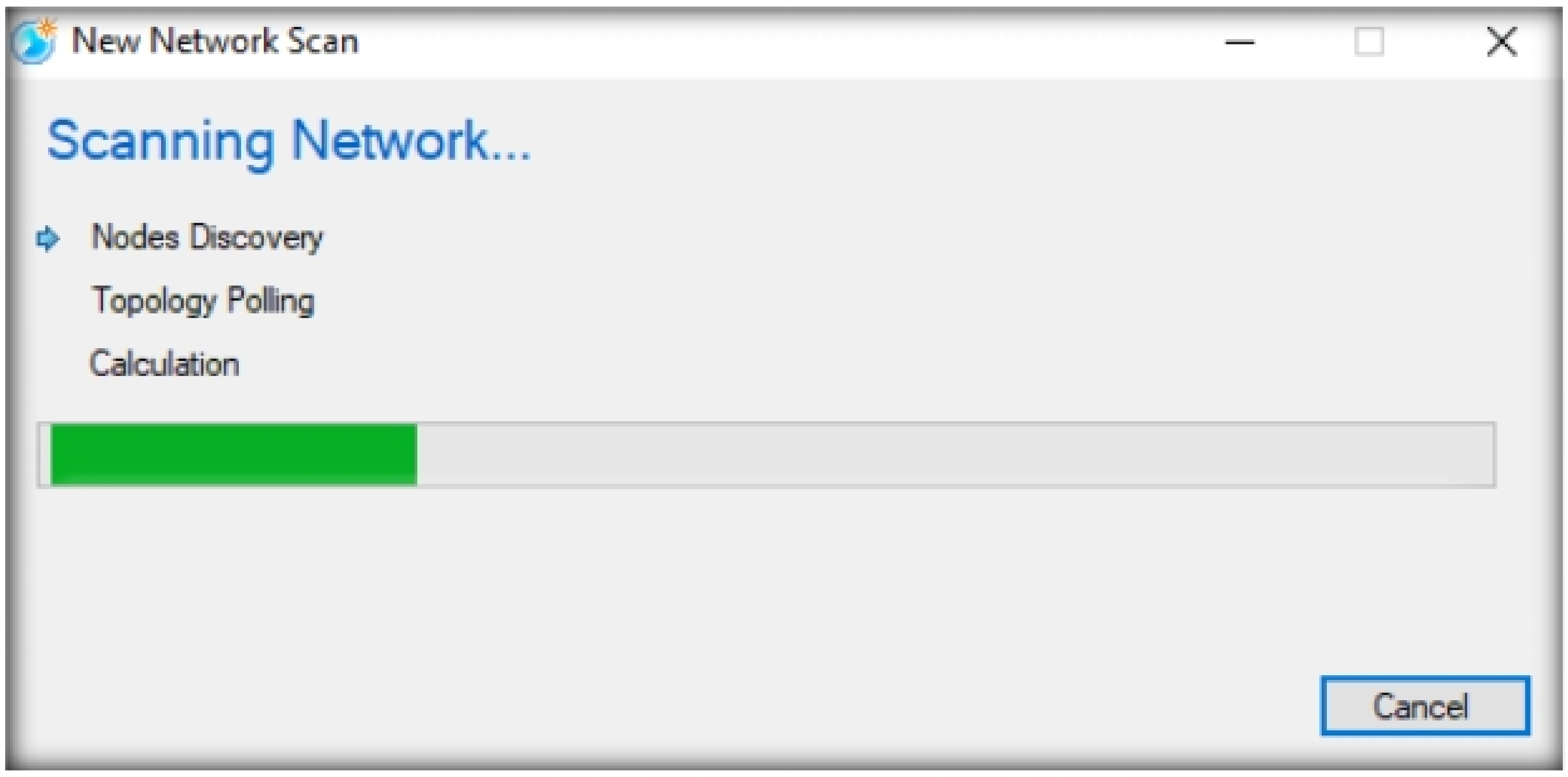
Scheduling:
Frequency: Once
Execution: Immediately

TIPS
- Network discovery can only draw connections between devices that have SNMP enabled. Non-SNMP devices cannot be mapped.
- Provide Windows and VMWare credentials for devices on your network.

solarwinds
SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary
< Back
Discover
Cancel

Figure 5.1.11: Summary section

17. The **New Network Scan** window appears; the Network Topology Mapper starts scanning the network for live hosts.



New Network Scan

Scanning Network...

Nodes Discovery

Topology Polling

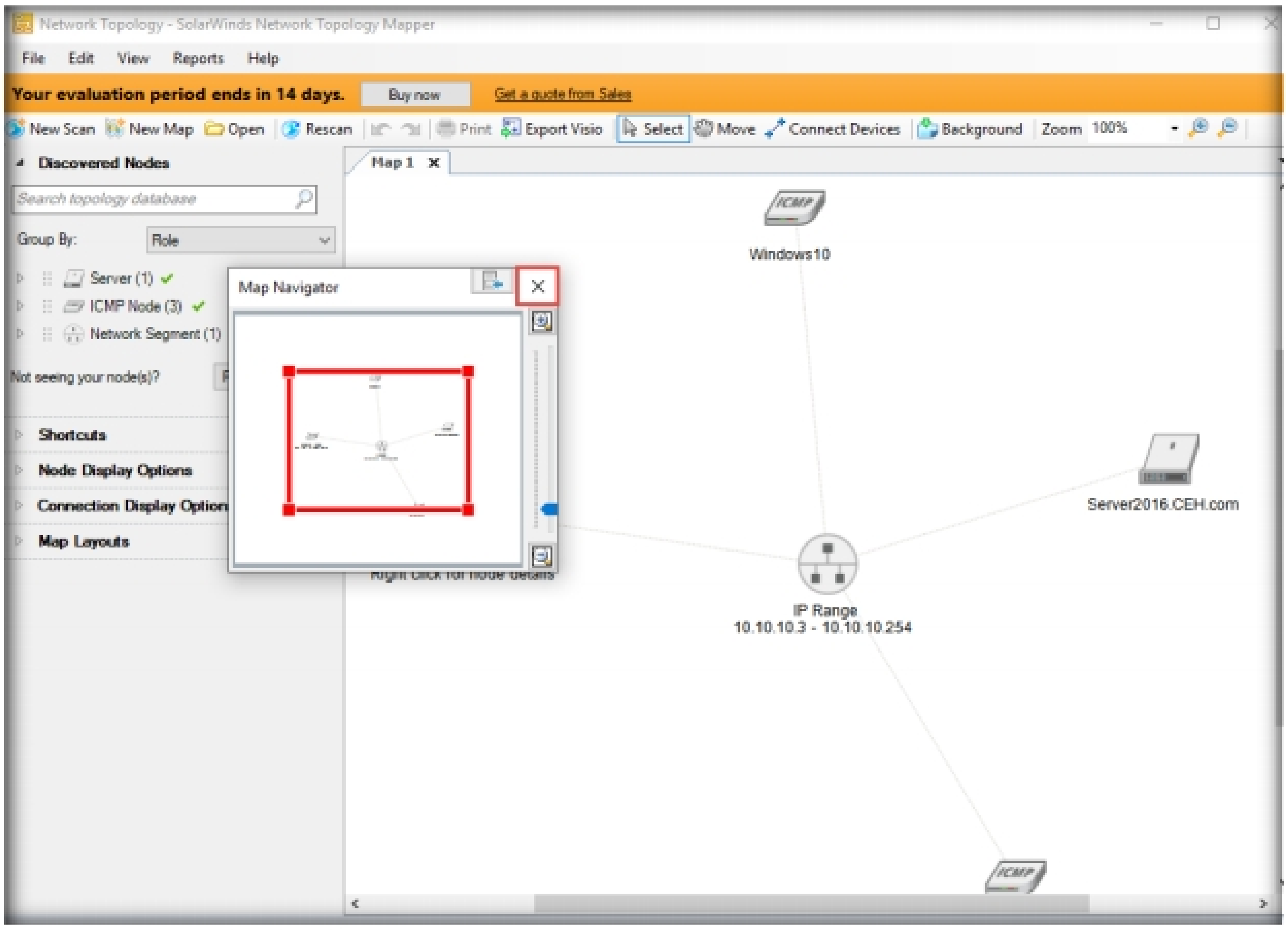
Calculation

Figure 5.1.12: Network Topology Mapper scanning the network

TASK 1.3

Draw Network Diagram

18. The **Network Topology - SolarWinds Network Topology Mapper** window appears. Close the **Map Navigator** window.



Your evaluation period ends in 14 days.

Network Topology - SolarWinds Network Topology Mapper
File
Edit
View
Reports
Help
Buy now
Get a quote from Sales
New Scan
New Map
Open
Rescan
Print
Export Visio
Select
Move
Connect Devices
Background
Zoom
100%
Discovered Nodes
Search topology database
Group By:
Role
Server (1)
ICMP Node (3)
Network Segment (1)
Not seeing your node(s)?
Shortcuts
Node Display Options
Connection Display Options
Map Layouts
Map 1
Map Navigator
ICMP
Windows10
Server2016.CEH.com
IP Range
10.10.10.3 - 10.10.10.254
ICMP

Figure 5.1.13: Network Scan results window

19. The **Network Topology Mapper** displays a network topology diagram for the provided IP address range, as shown in the following screenshot.

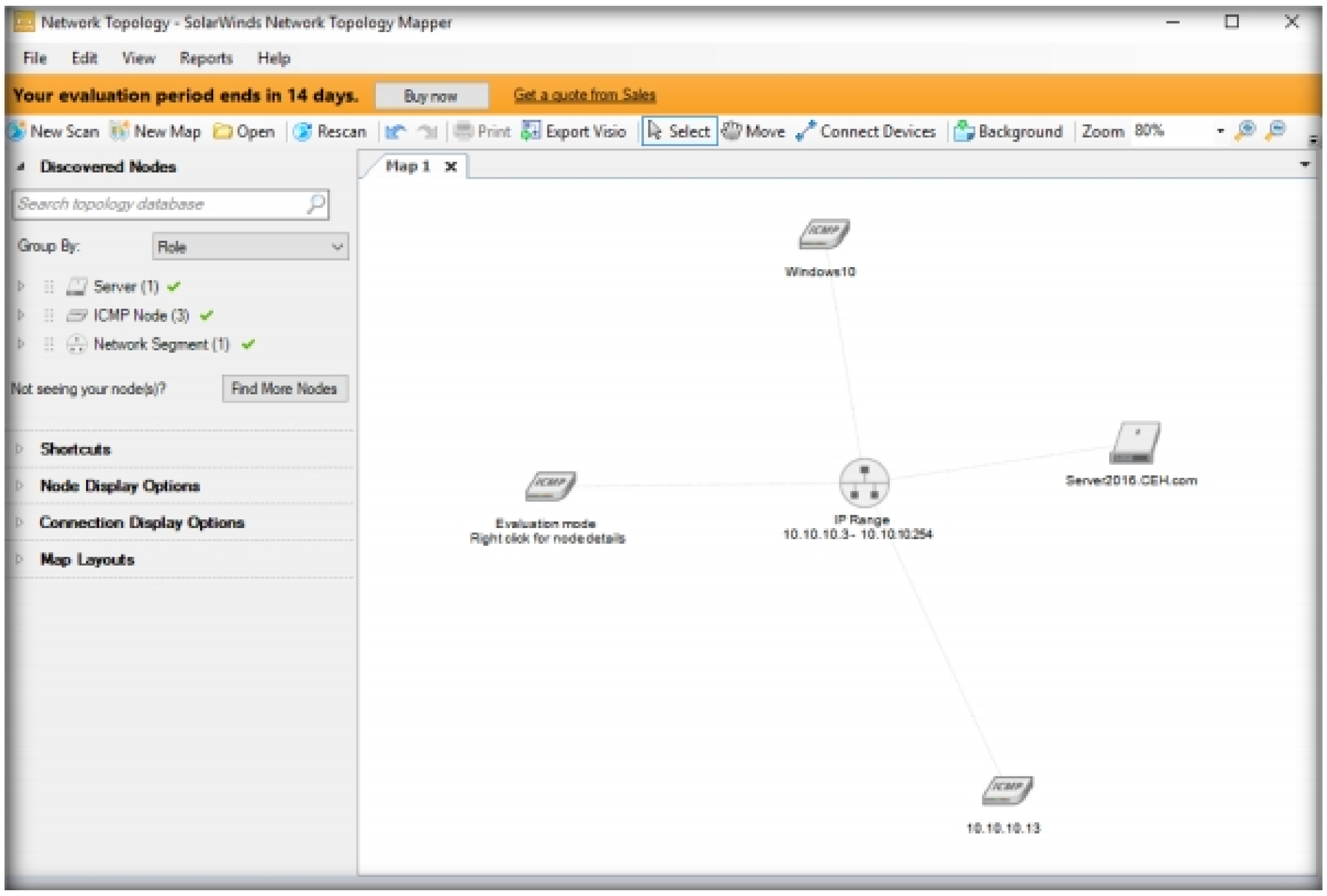

Network Topology - SolarWinds Network Topology Mapper
File Edit View Reports Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Scan
New Map
Open
Rescan
Print
Export Visio
Select
Move
Connect Devices
Background
Zoom 80%
Discovered Nodes
Search topology database
Group By: Role
Server (1)
ICMP Node (3)
Network Segment (1)
Not seeing your node(s)?
Find More Nodes
Shortcuts
Node Display Options
Connection Display Options
Map Layouts
Map 1
Windows10
Server2016.CEH.com
Evaluation mode
Right click for node details
IP Range
10.10.10.3 - 10.10.10.254
10.10.10.13

Figure 5.1.14: Network topology diagram

20. Expand **Node Display Options** in the right-hand pane and select the **IP address** checkbox. This displays IP addresses for all nodes in the layout.

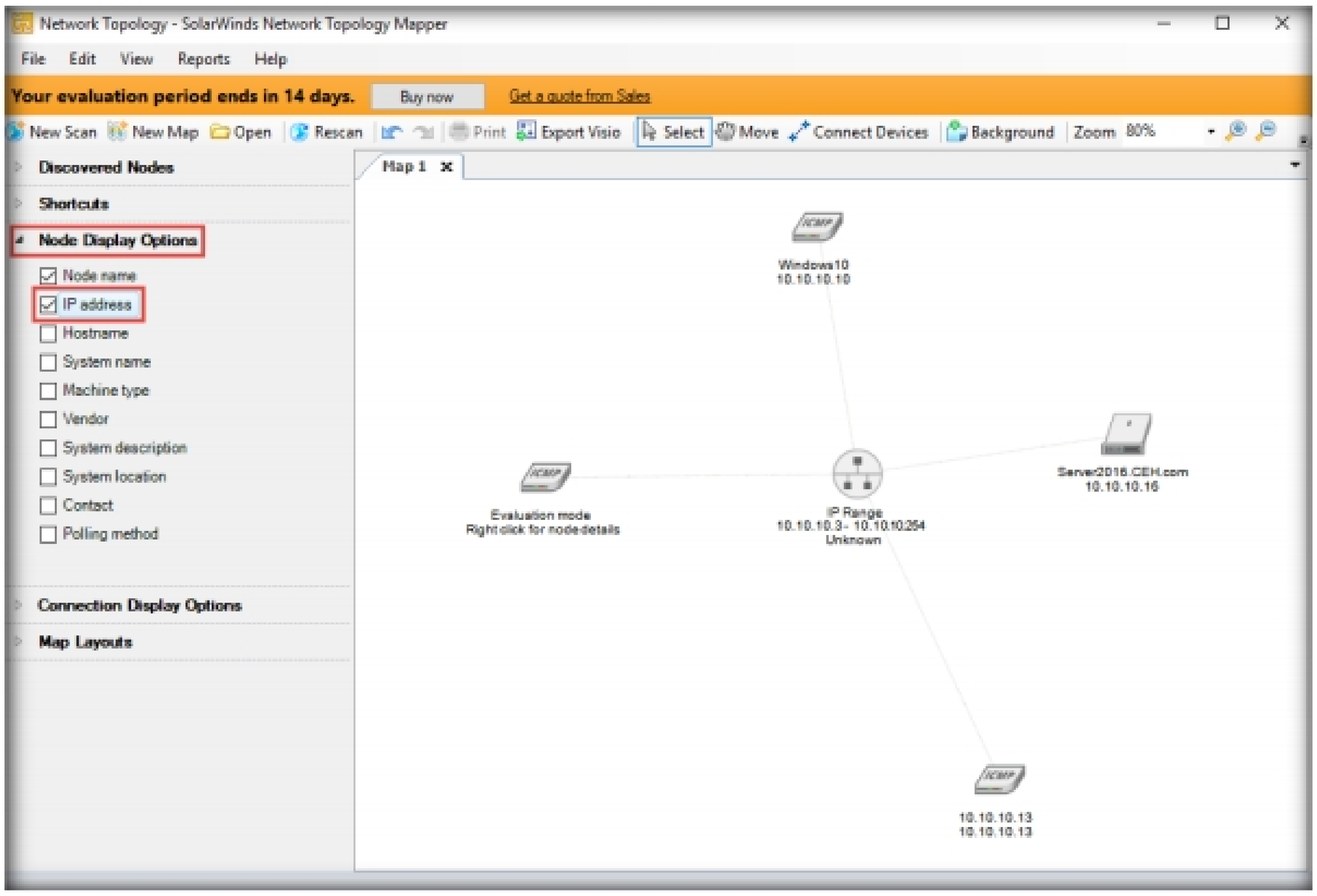

Network Topology - SolarWinds Network Topology Mapper
File Edit View Reports Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Scan
New Map
Open
Rescan
Print
Export Visio
Select
Move
Connect Devices
Background
Zoom 80%
Discovered Nodes
Shortcuts
Node Display Options
☑ Node name
☑ IP address
☐ Hostname
☐ System name
☐ Machine type
☐ Vendor
☐ System description
☐ System location
☐ Contact
☐ Polling method
Connection Display Options
Map Layouts
Map 1
Windows10
10.10.10.10
Server2016.CEH.com
10.10.10.16
Evaluation mode
Right click for node details
IP Range
10.10.10.3 - 10.10.10.254
Unknown
10.10.10.13
10.10.10.13

Figure 5.1.15: Node Display Options: selecting the IP address

21. Now, expand the **Map Layouts** node, and select **Symmetrical** under the **Auto Arrange** section to change the topology layout of the mapped network. Each time you click **Symmetrical**, all nodes are rearranged randomly.

Note: You may select the node display options of your choice: whichever options you choose, they are added to the topology map. These topology maps are saved automatically to **C:\ProgramData\Solarwinds\Network Topology Mapper\UserMaps**.

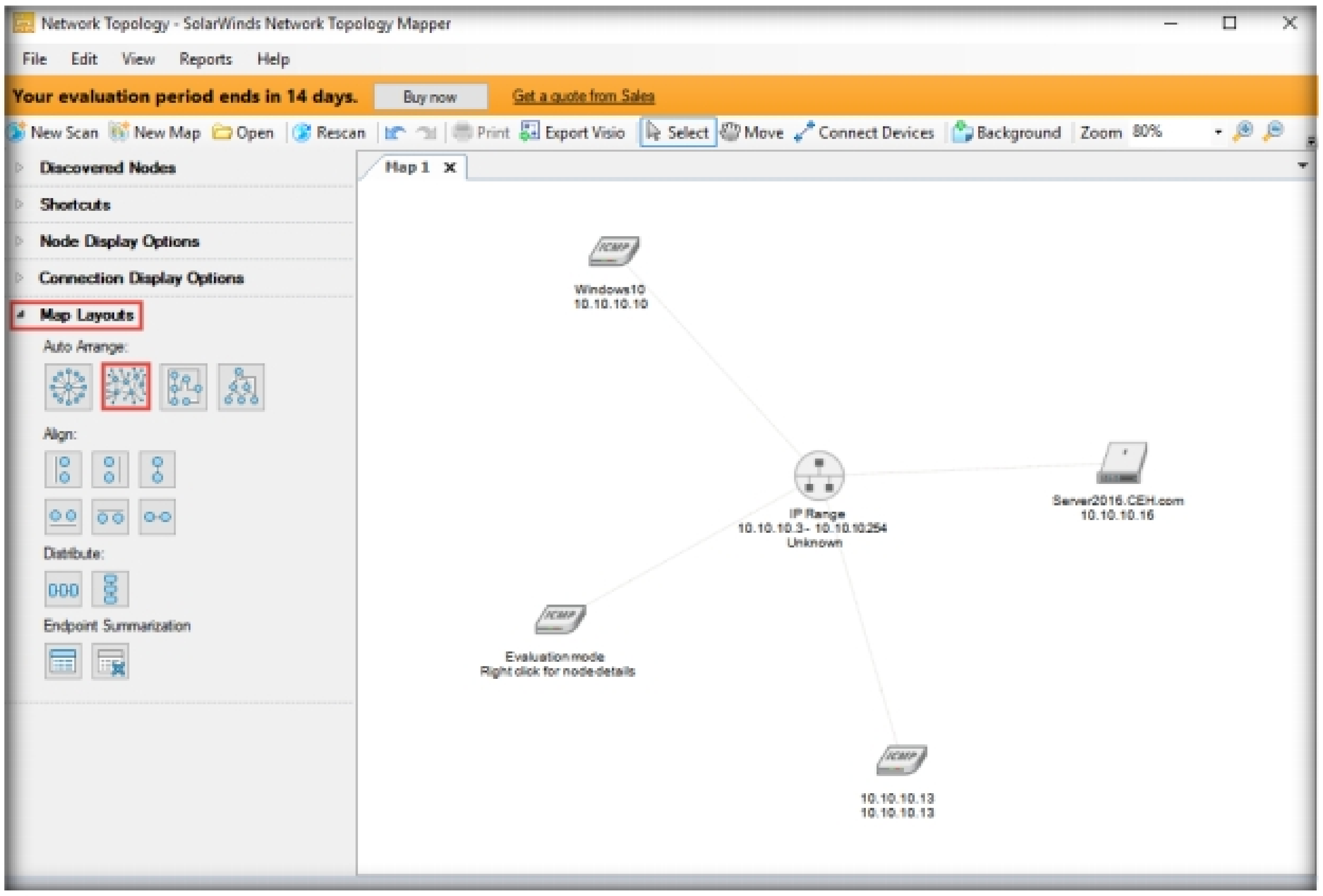

Network Topology - SolarWinds Network Topology Mapper
File
Edit
View
Reports
Help
Your evaluation period ends in 14 days.
Buy now
Get a quote from Sales
New Scan
New Map
Open
Rescan
Print
Export Visio
Select
Move
Connect Devices
Background
Zoom 80%
Discovered Nodes
Shortcuts
Node Display Options
Connection Display Options
Map Layouts
Auto Arrange:
Align:
Distribute:
Endpoint Summarization
Map 1
Windows10
10.10.10.10
IP Range
10.10.10.3 - 10.10.10.254
Unknown
Server2016.CEH.com
10.10.10.16
Evaluation mode
Right click for node details
10.10.10.13
10.10.10.13

Figure 5.1.16: Map Layouts Options: selecting Symmetrical

22. Right-click on a node (here **Server2016** with IP address **10.10.10.16**) and select **Node Properties** to view information about the selected node.

Note: The network diagram and the IP addresses might differ in your lab environment

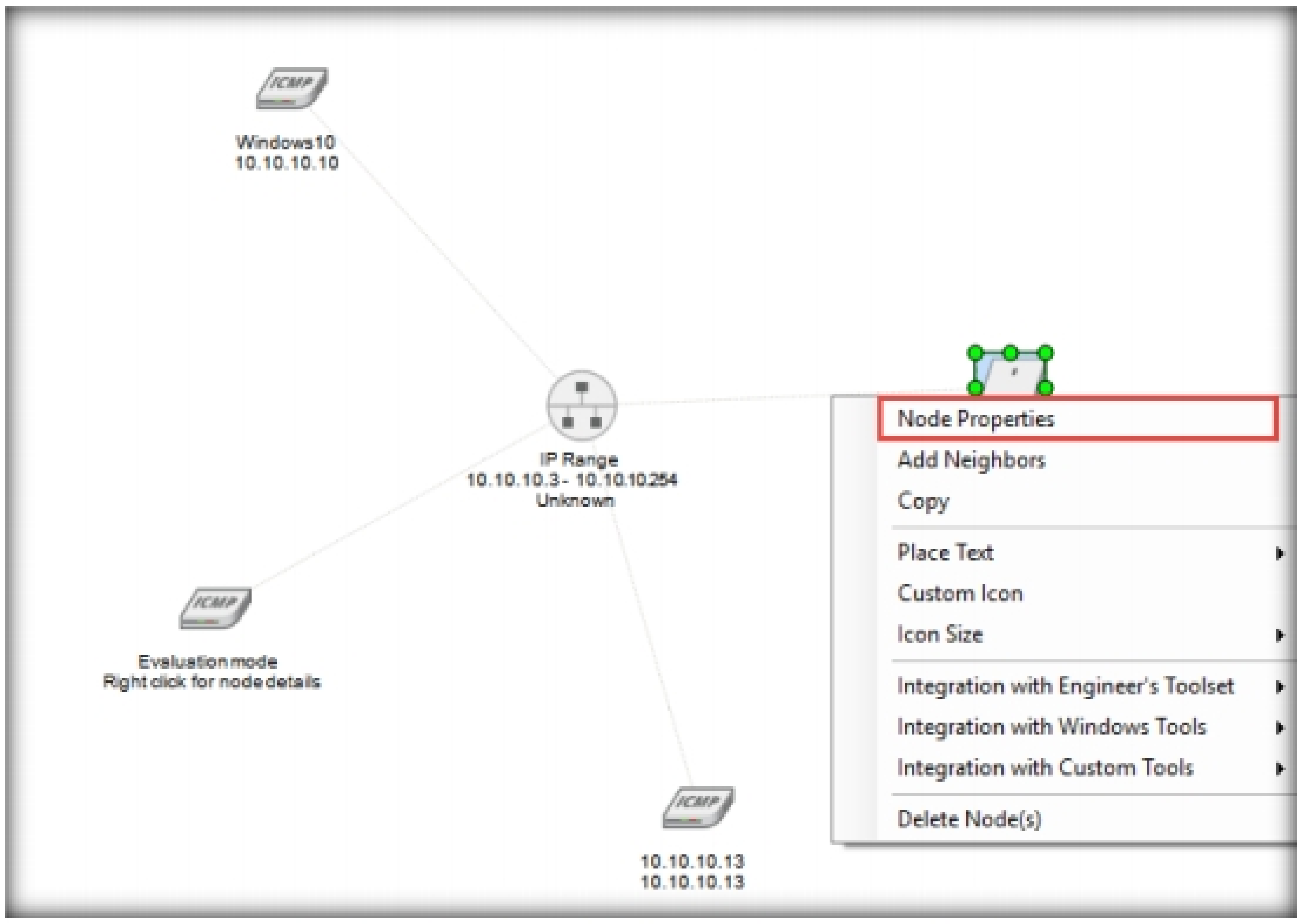
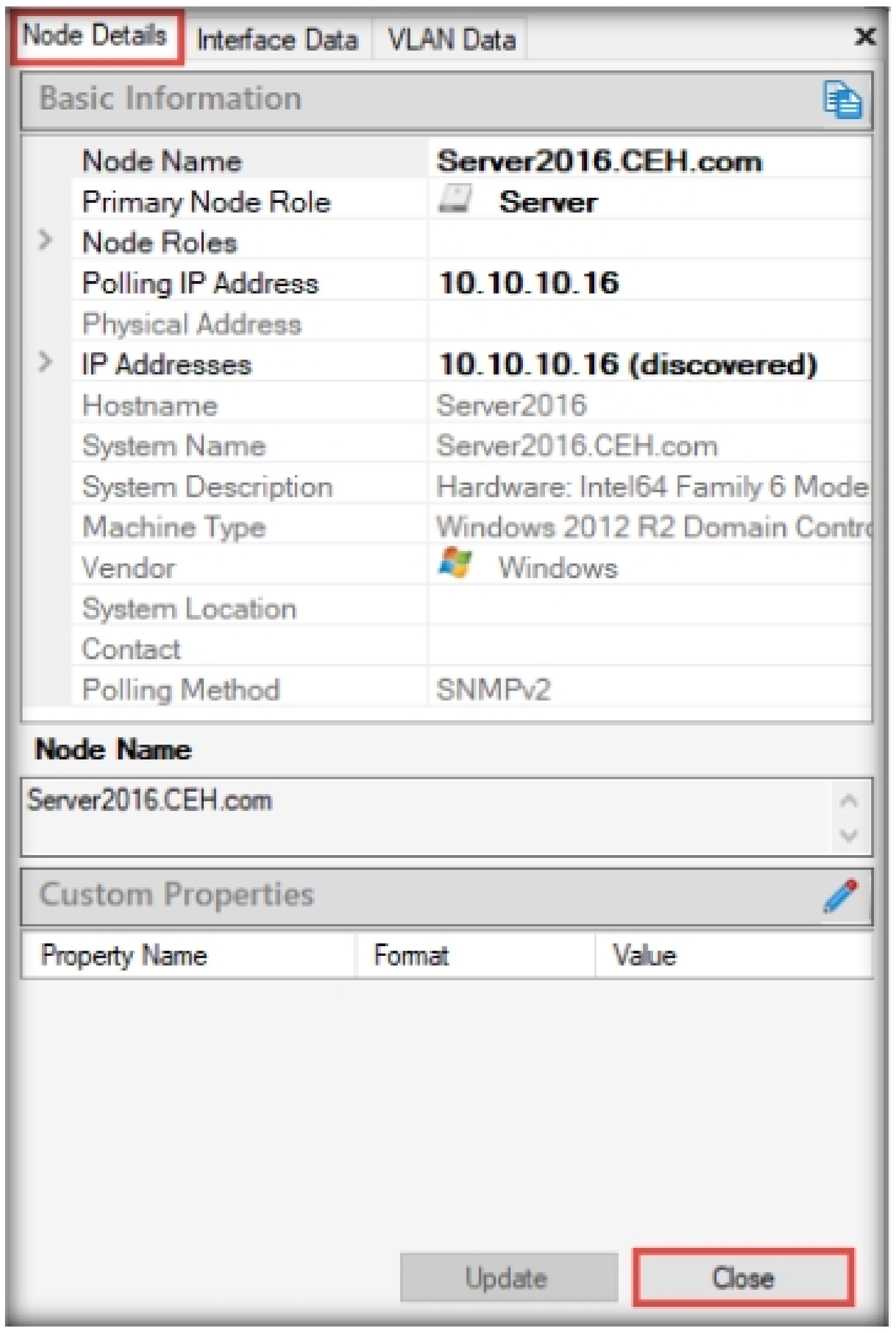

Windows10
10.10.10.10
IP Range
10.10.10.3 - 10.10.10.254
Unknown
Evaluation mode
Right click for node details
10.10.10.13
10.10.10.13
Node Properties
Add Neighbors
Copy
Place Text
Custom Icon
Icon Size
Integration with Engineer's Toolset
Integration with Windows Tools
Integration with Custom Tools
Delete Node(s)

Figure 5.1.17: Viewing the details of a selected target machine

23. The **Node Details** window appears, displaying information about the selected node. Click **Close** to close the window.



Node Details
Interface Data
VLAN Data
×
Basic Information

Node Name	Server2016.CEH.com
Primary Node Role	Server
Node Roles	
Polling IP Address	10.10.10.16
Physical Address	
IP Addresses	10.10.10.16 (discovered)
Hostname	Server2016
System Name	Server2016.CEH.com
System Description	Hardware: Intel64 Family 6 Mode
Machine Type	Windows 2012 R2 Domain Contr
Vendor	Windows
System Location	
Contact	
Polling Method	SNMPv2

Node Name

Server2016.CEH.com

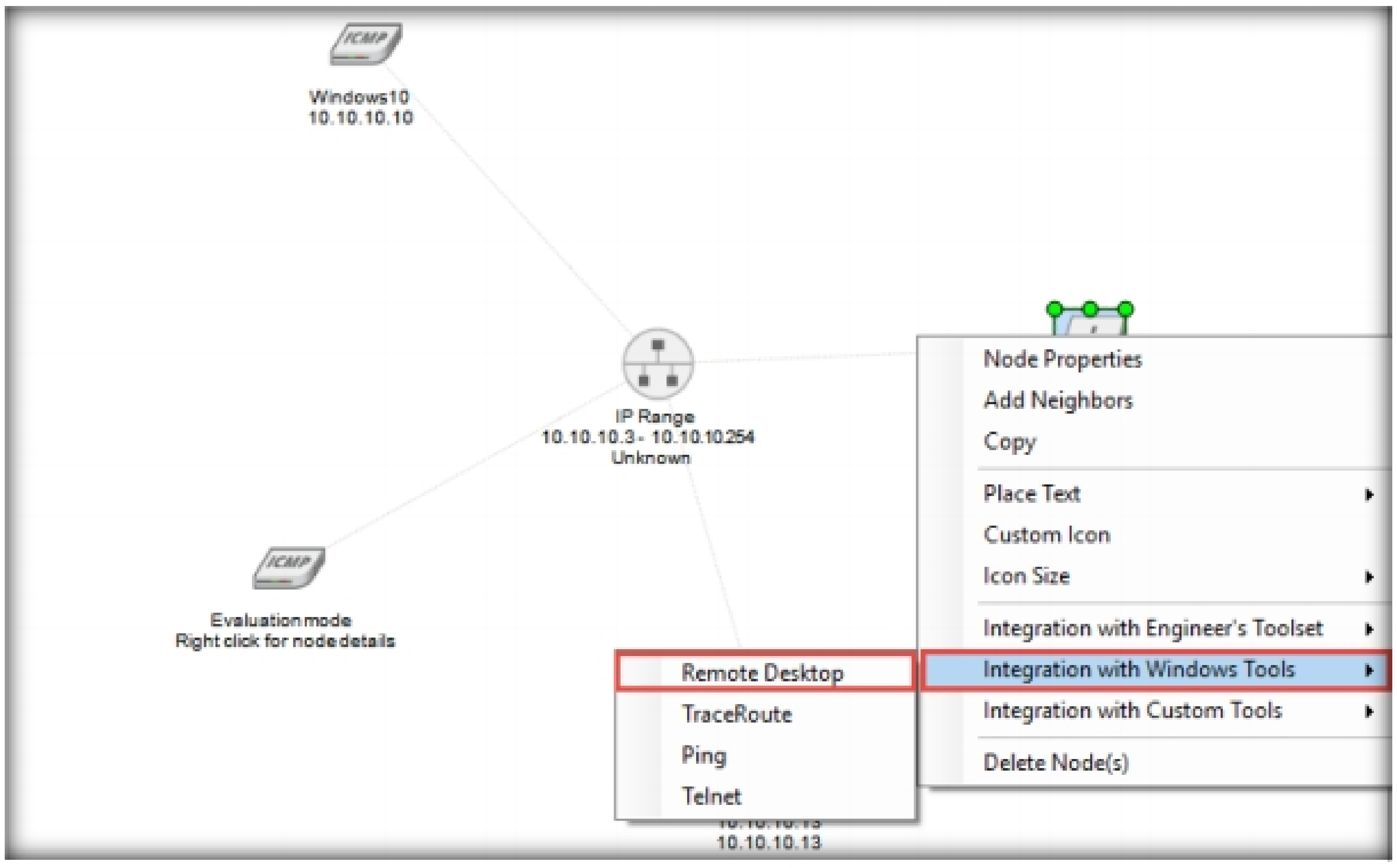
Custom Properties
Property Name
Format
Value
Update
Close

Figure 5.1.18: Details window

TASK 1.4

Additional Features in Network Topology Mapper

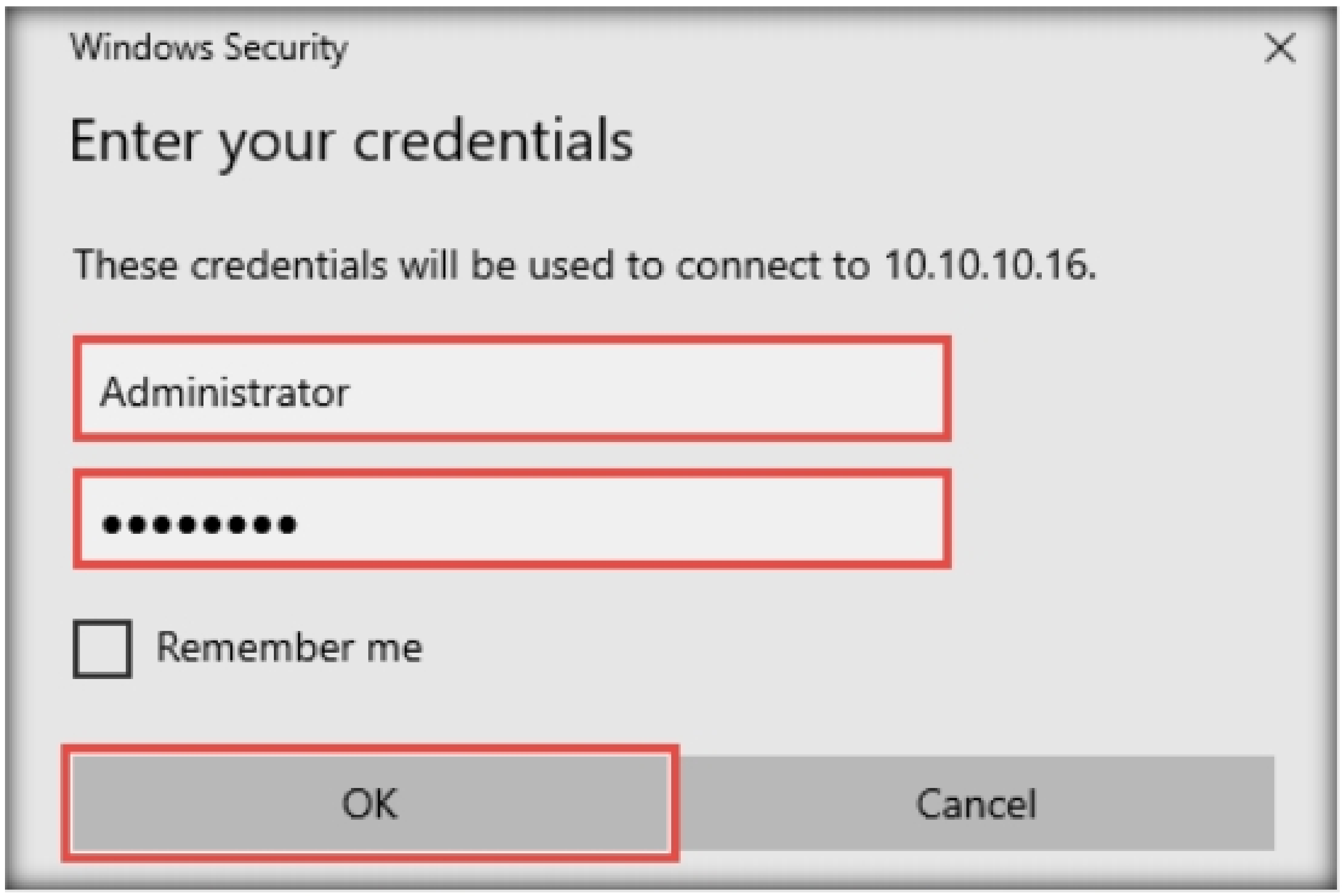
24. Right-click on a node (**Server2016** with IP address **10.10.10.16**) and select **Integration with Windows Tools** and click **Remote Desktop**.



ICMP
Windows10
10.10.10.10
IP Range
10.10.10.3 - 10.10.10.254
Unknown
ICMP
Evaluation mode
Right click for node details
Node Properties
Add Neighbors
Copy
Place Text
Custom Icon
Icon Size
Integration with Engineer's Toolset
Integration with Windows Tools
Integration with Custom Tools
Delete Node(s)
Remote Desktop
TraceRoute
Ping
Telnet
10.10.10.13

Figure 5.1.19: Establishing a Remote Desktop Connection with the target machine

25. The **Windows Security** dialog box appears. Enter **Username** as **Administrator** and **Password** as **Pa$$w0rd** for **Windows Server 2016**, and click **OK**.



Windows Security

Enter your credentials

These credentials will be used to connect to 10.10.10.16.

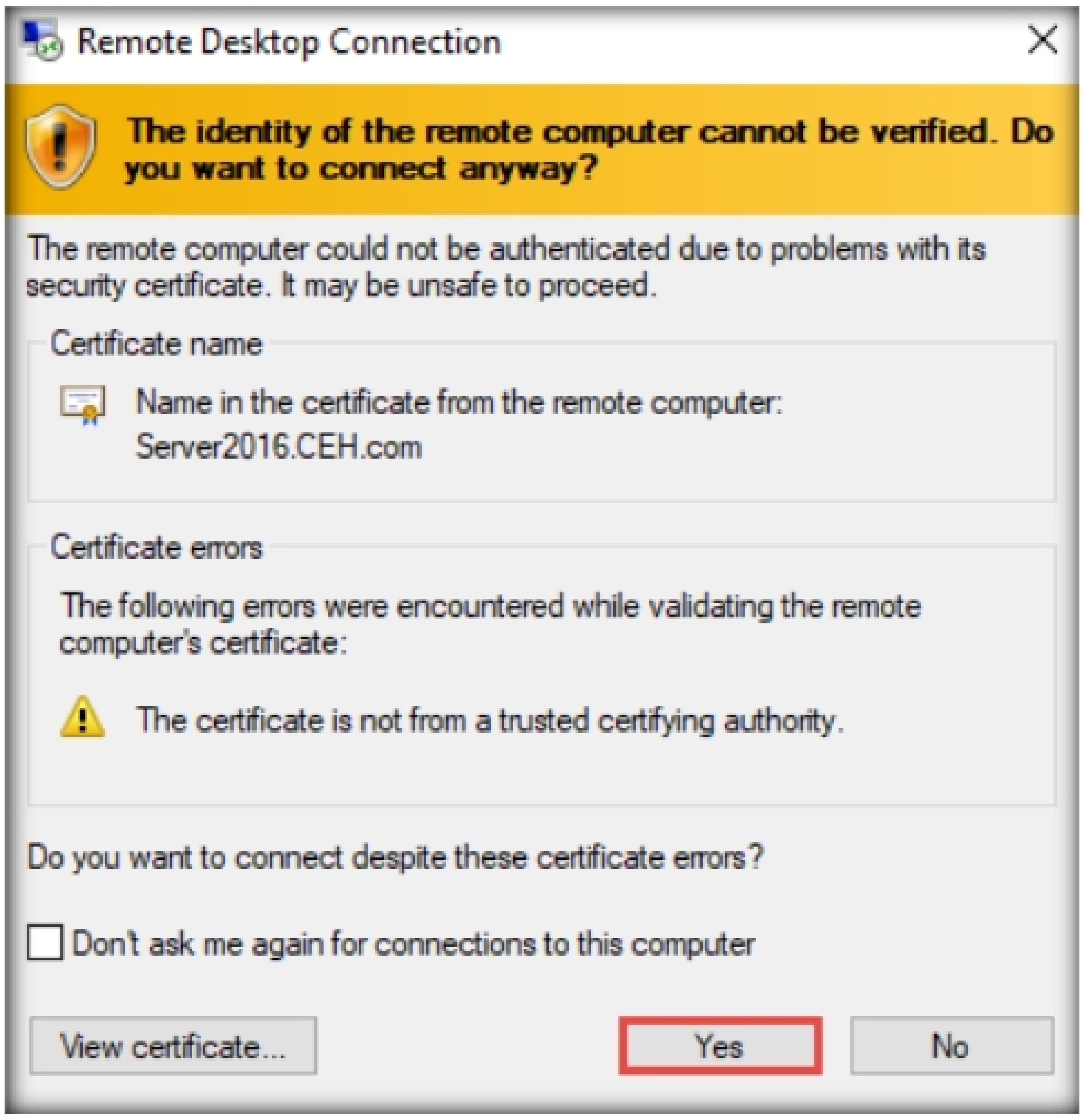
Administrator

●●●●●●●●

☐ Remember me

Figure 5.1.20: Establishing a Remote Desktop Connection with the target machine

26. The **Remote Desktop Connection** pop-up appears; click **Yes**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Server2016.CEH.com

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

☐ Don't ask me again for connections to this computer

Figure 5.1.21: Establishing a remote desktop connection with the target machine

27. The **Remote Desktop Connection** is successfully set to the target virtual machine (here, **Windows Server 2016**), as shown in the following screenshot.

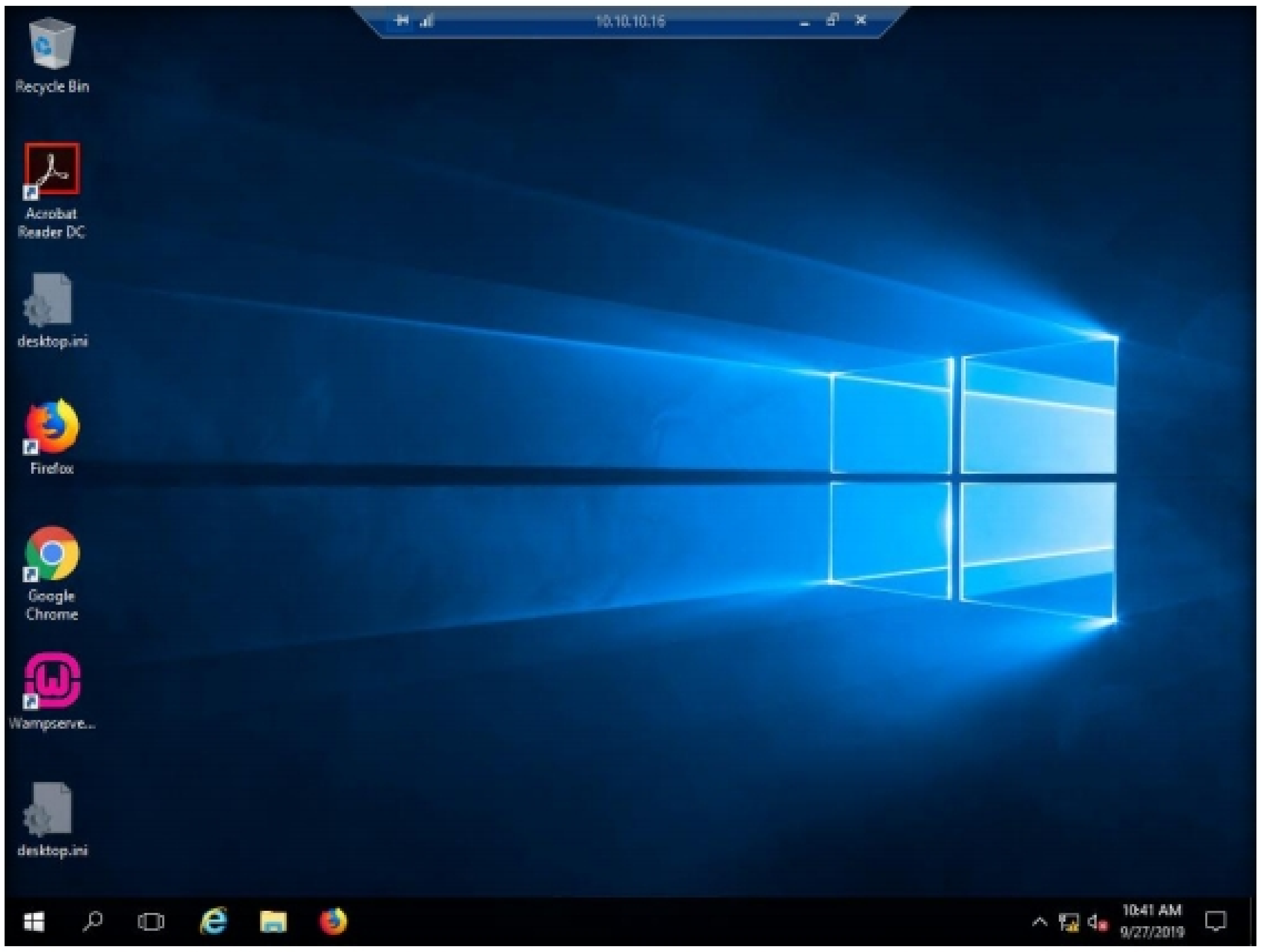


Figure 5.1.22: Remote Desktop Connection established with the target machine

You can also use other network discovery tools such as **OpManager** (https://www.manageengine.com), **The Dude** (https://mikrotik.com), **NetSurveyor** (http://nutsaboutnets.com), **NetBrain** (https://www.netbraintech.com), and **Spiceworks Network Mapping Tool** (https://www.spiceworks.com) to draw network diagram of the target network.

28. You can use other options such as **Ping**, **Telnet**, and **Traceroute**. Similarly, an attacker can use this application to draw network diagrams, find the active hosts on the network, perform Ping, Telnet, etc.

29. This concludes the demonstration of drawing network diagram of the target network using Network Topology Mapper.

30. Close all open windows and document all the acquired information.

31. Turn off all the virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
6

Perform Network Scanning using Various Scanning Tools

Ethical hackers and pen testers are aided in network scanning with the help of various scanning tools, which make scanning a target network an easy task.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks**

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Lab Tasks

TASK 1

Scan a Target Network using Metasploit

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

TASK 1.1

Link Metasploit Framework to Database

1. Before starting this task, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machine.
2. Switch to the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

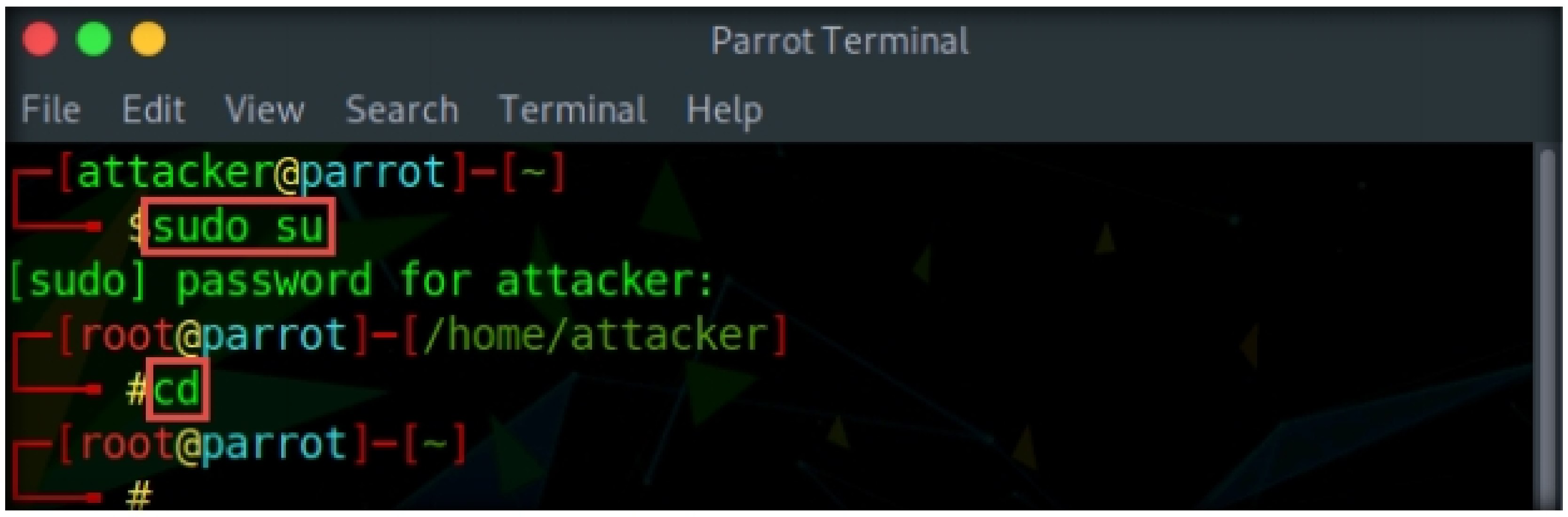
- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

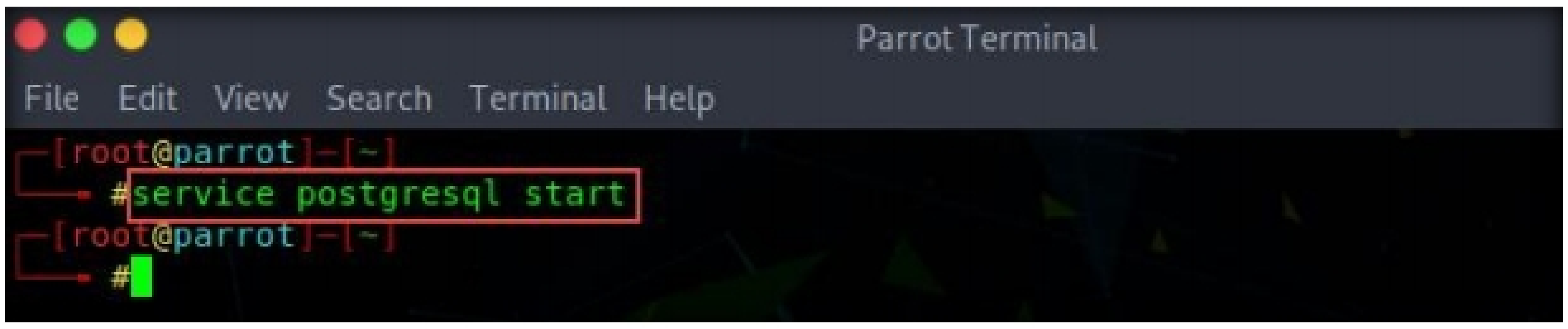
7. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 6.1.1: Running the programs as a root user

8. In the **Parrot Terminal** window, type **service postgresql start** and hit **Enter**.

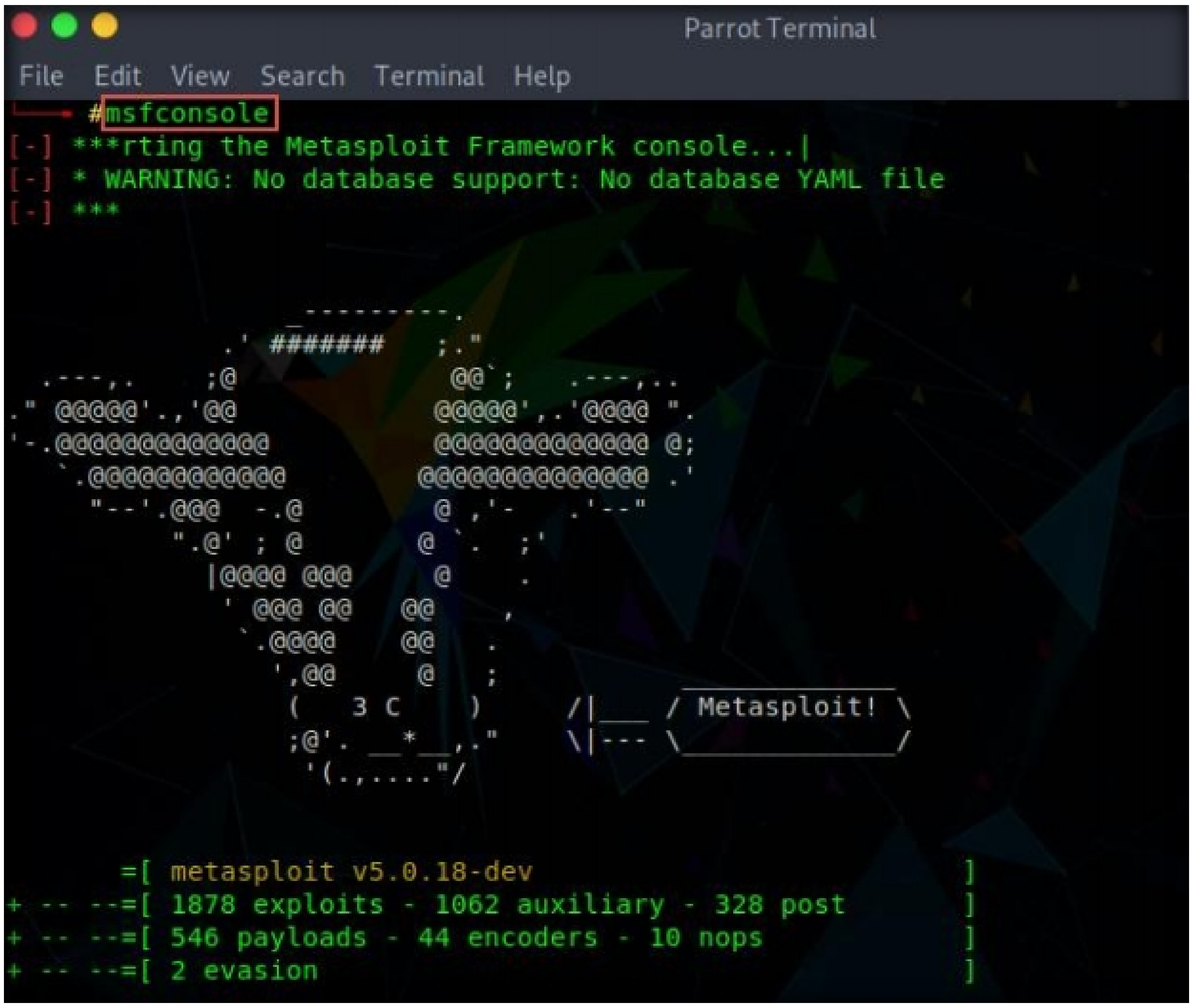

Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #service postgresql start
┌─[root@parrot]─[~]
└──╼ #
```

Figure 6.1.2: Start postgresql service through the command line

9. Now, type **msfconsole** and hit **Enter** to launch Metasploit.

Note: The version of Metasploit might differ in your lab environment.

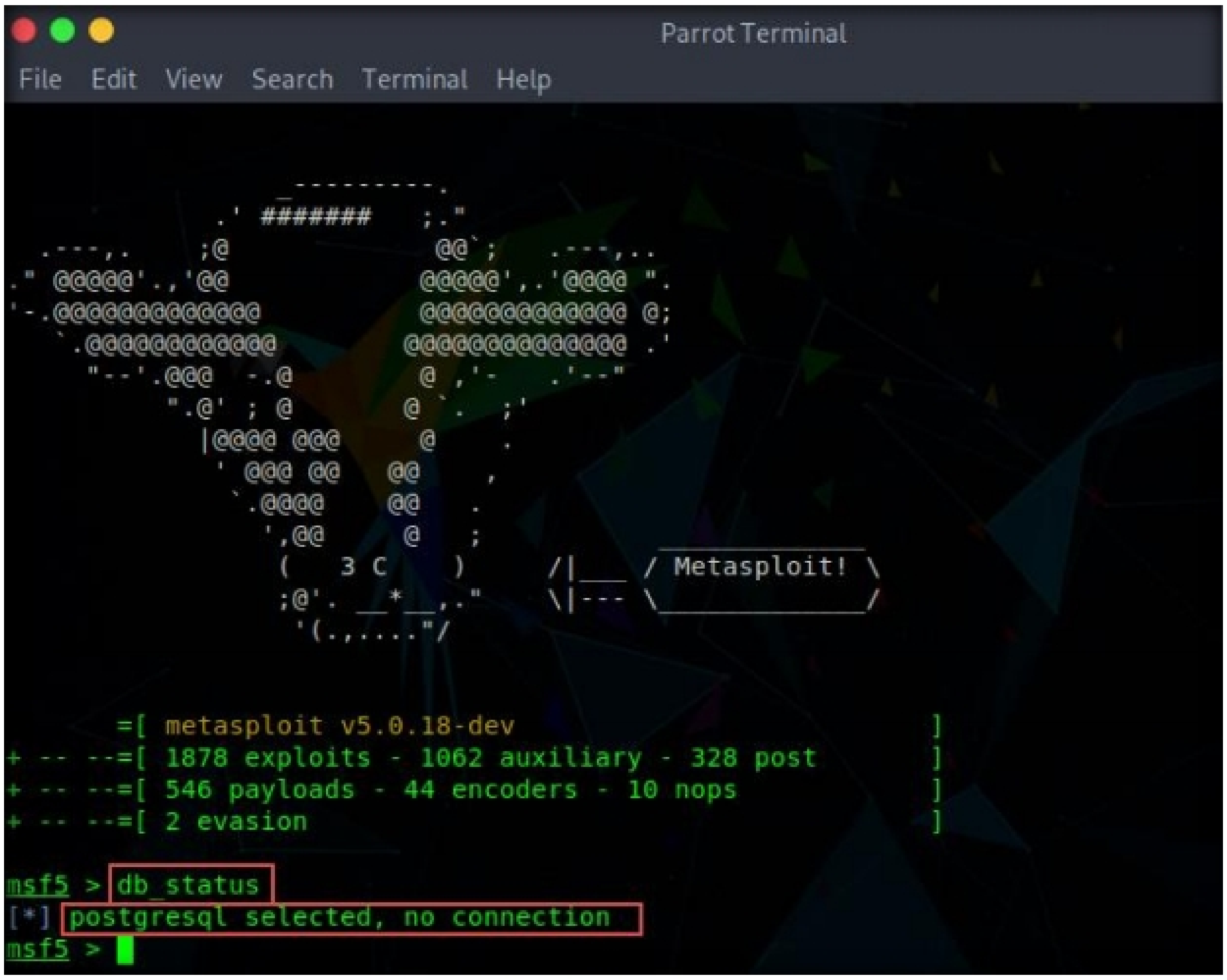

Parrot Terminal
File Edit View Search Terminal Help

```
└──╼ #msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***


                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@   -.@       @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ metasploit v5.0.18-dev                         ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops           ]
+ -- --=[ 2 evasion                                       ]
```

Figure 6.1.3: Launch Metasploit framework

10. An msf command line appears. Type **db_status** and hit **Enter** to check if Metasploit has connected to the database successfully. If you receive the message "**postgersql selected, no connection**," then the database did not connect to msf.

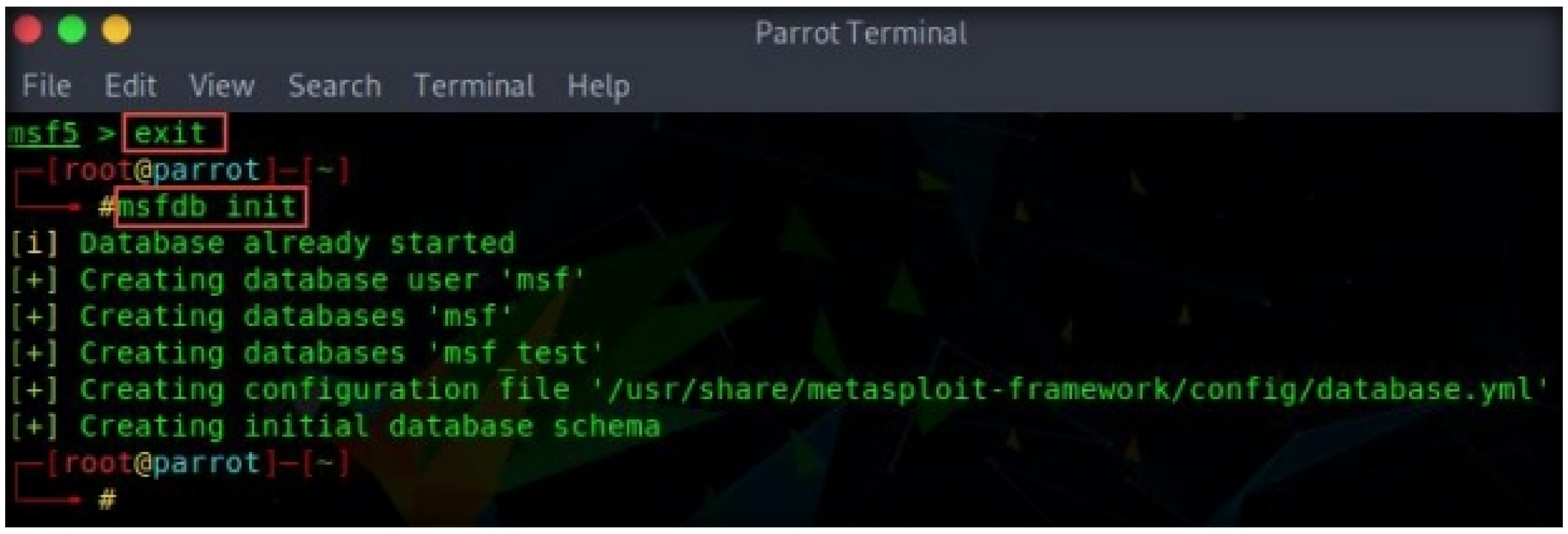
Note: If the message you receive is "**connected to msf**," then skip to **Step #14**.



```
                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ metasploit v5.0.18-dev                          ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > db_status
[*] postgresql selected, no connection
msf5 > 
```

Figure 6.1.4: Database not connected to msf

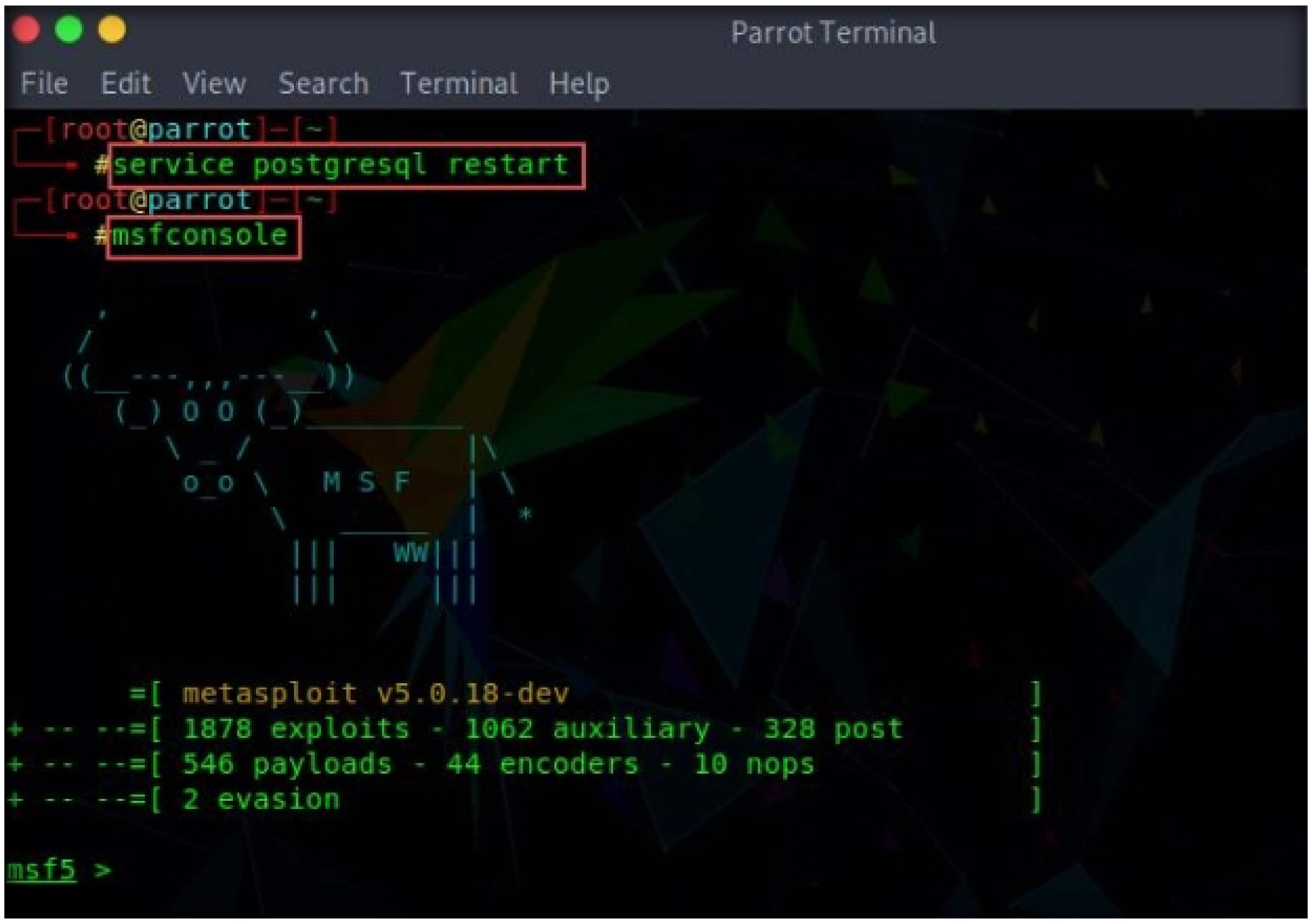
11. Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.



```
msf5 > exit
┌─[root@parrot]─[~]
└──╼ #msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
┌─[root@parrot]─[~]
└──╼ #
```

Figure 6.1.5: Initialize the database

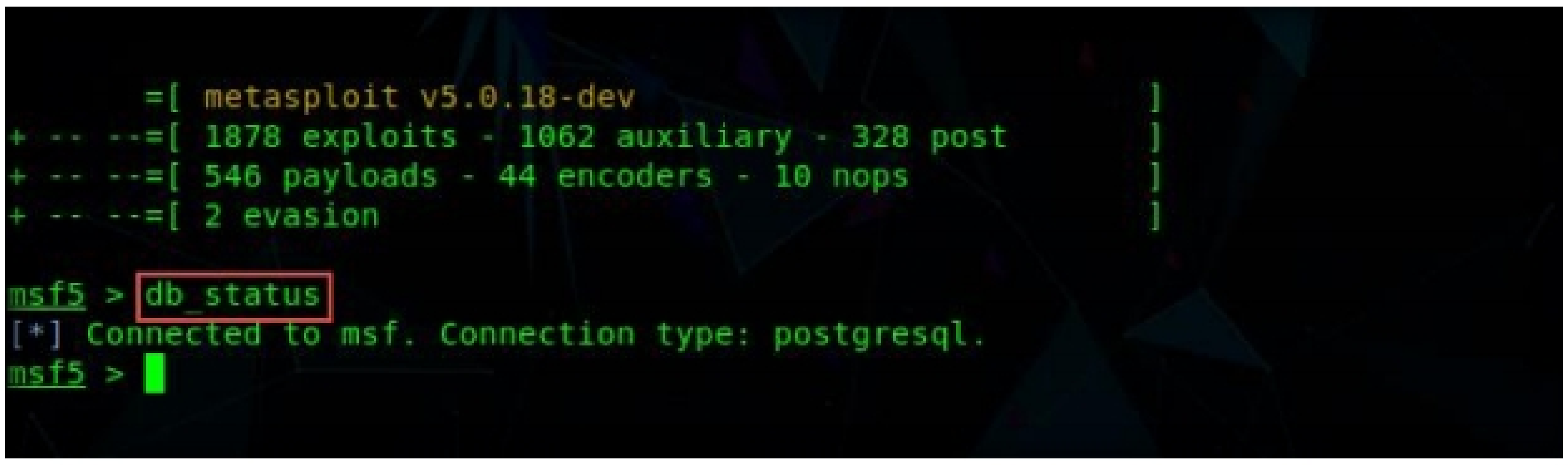
12. To restart the postgresql service, type **service postgresql restart** and press **Enter**. Now, start the Metasploit Framework again by typing **msfconsole** and pressing **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #service postgresql restart
┌─[root@parrot]─[~]
└──╼ #msfconsole

                 ,           ,
                /             \
               ((__---,,,---__))
                  (_) O O (_)_________
                     \ _ /            |\
                      o_o \   M S F   | \
                           \   _____  |  *
                            |||   WW|||
                            |||     |||


       =[ metasploit v5.0.18-dev                          ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 >
```

Figure 6.1.6: Launch Metasploit framework

13. Check the database status by typing **db_status** and press **Enter**. This time, the database should successfully connect to msf, as shown in the screenshot.



```
       =[ metasploit v5.0.18-dev                          ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```

Figure 6.1.7: Verify that database is successfully connected to Metasploit framework

TASK 1.2

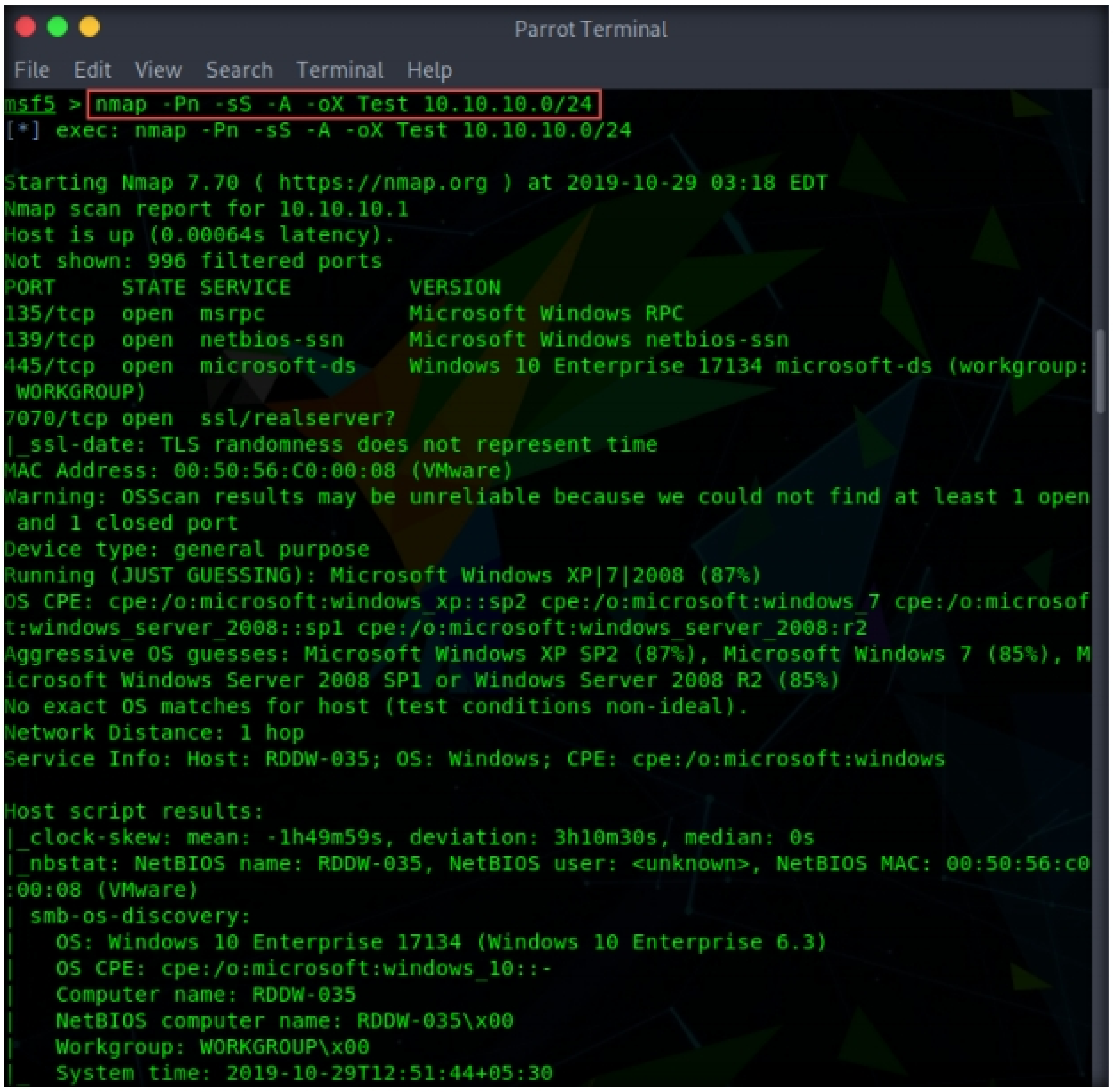
Information Gathering Using Metasploit

14. Type **nmap -Pn -sS -A -oX Test 10.10.10.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

Here, we are scanning the whole subnet 10.10.10.0/24 for active hosts.

Note: The target IP address subnet might differ in your lab environment.

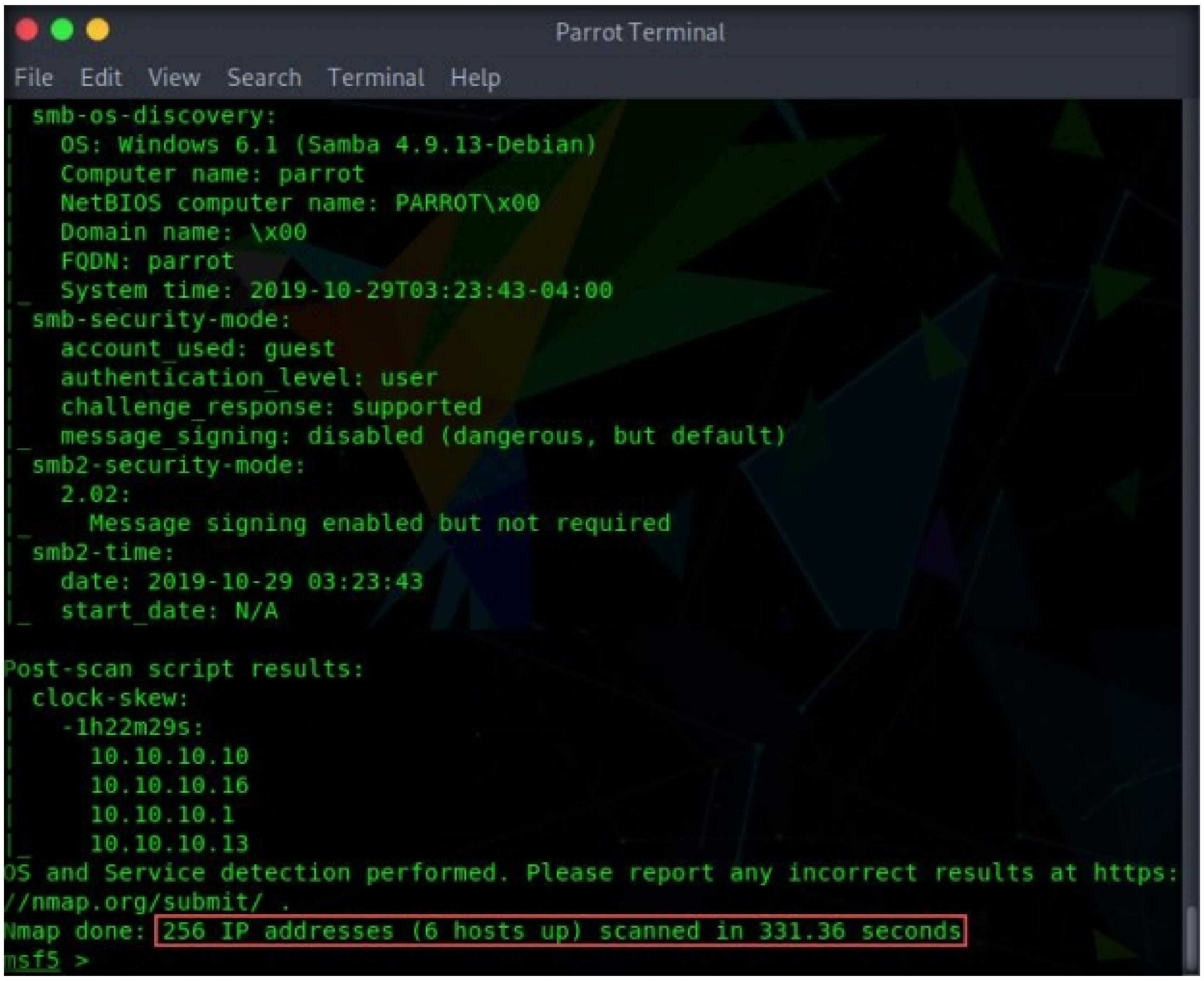
15. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.



```
msf5 > nmap -Pn -sS -A -oX Test 10.10.10.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.10.0/24

Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-29 03:18 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00064s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds    Windows 10 Enterprise 17134 microsoft-ds (workgroup:
 WORKGROUP)
7070/tcp open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
 and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsof
t:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), M
icrosoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: RDDW-035; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 3h10m30s, median: 0s
|_nbstat: NetBIOS name: RDDW-035, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0
:00:08 (VMware)
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: RDDW-035
|   NetBIOS computer name: RDDW-035\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-10-29T12:51:44+05:30
```

Figure 6.1.8: Nmap scan result

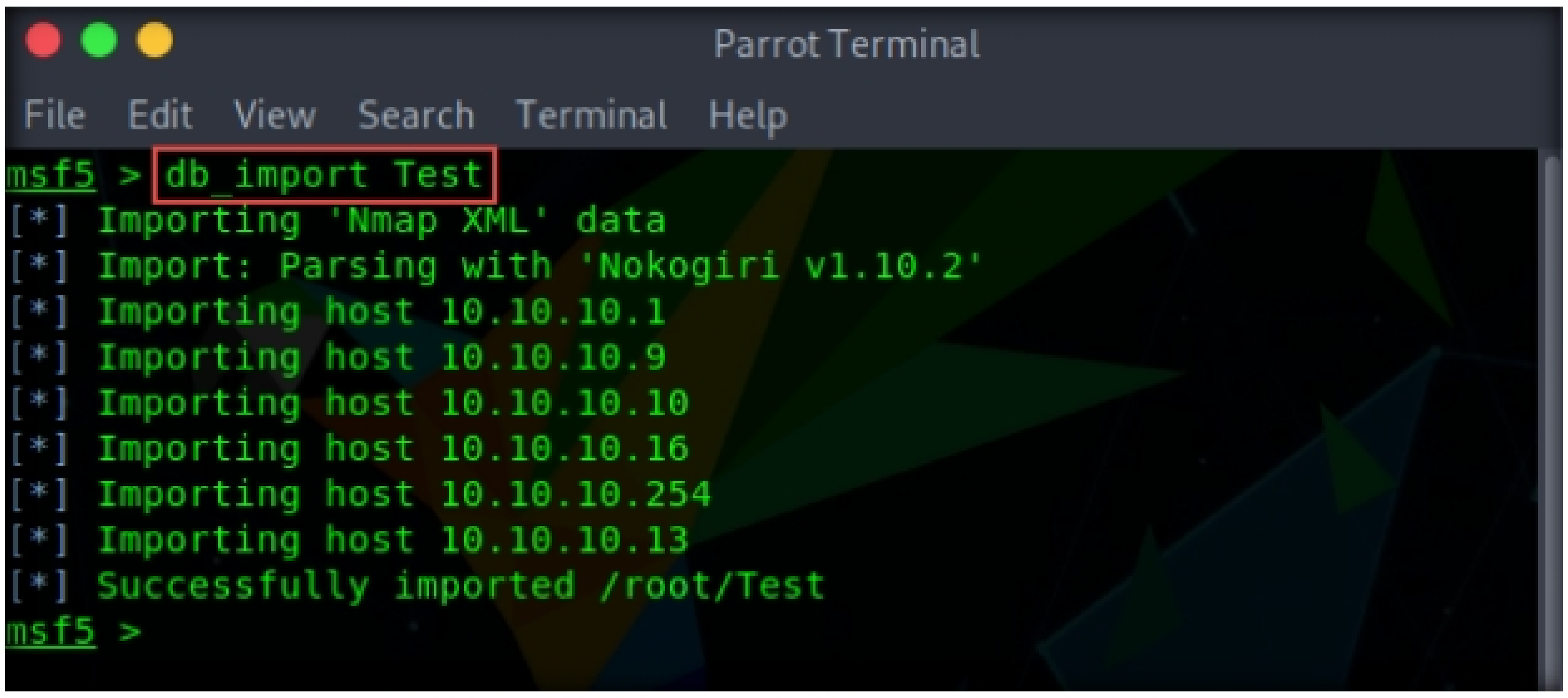
16. After the scan completes, Nmap displays the number of active hosts in the target network (here, **6**).



```
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.13-Debian)
|   Computer name: parrot
|   NetBIOS computer name: PARROT\x00
|   Domain name: \x00
|   FQDN: parrot
|_  System time: 2019-10-29T03:23:43-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-10-29 03:23:43
|_  start_date: N/A

Post-scan script results:
| clock-skew:
|   -1h22m29s:
|     10.10.10.10
|     10.10.10.16
|     10.10.10.1
|_    10.10.10.13
OS and Service detection performed. Please report any incorrect results at https:
//nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 331.36 seconds
msf5 >
```

Figure 6.1.9: Nmap showing new found hosts in the subnet

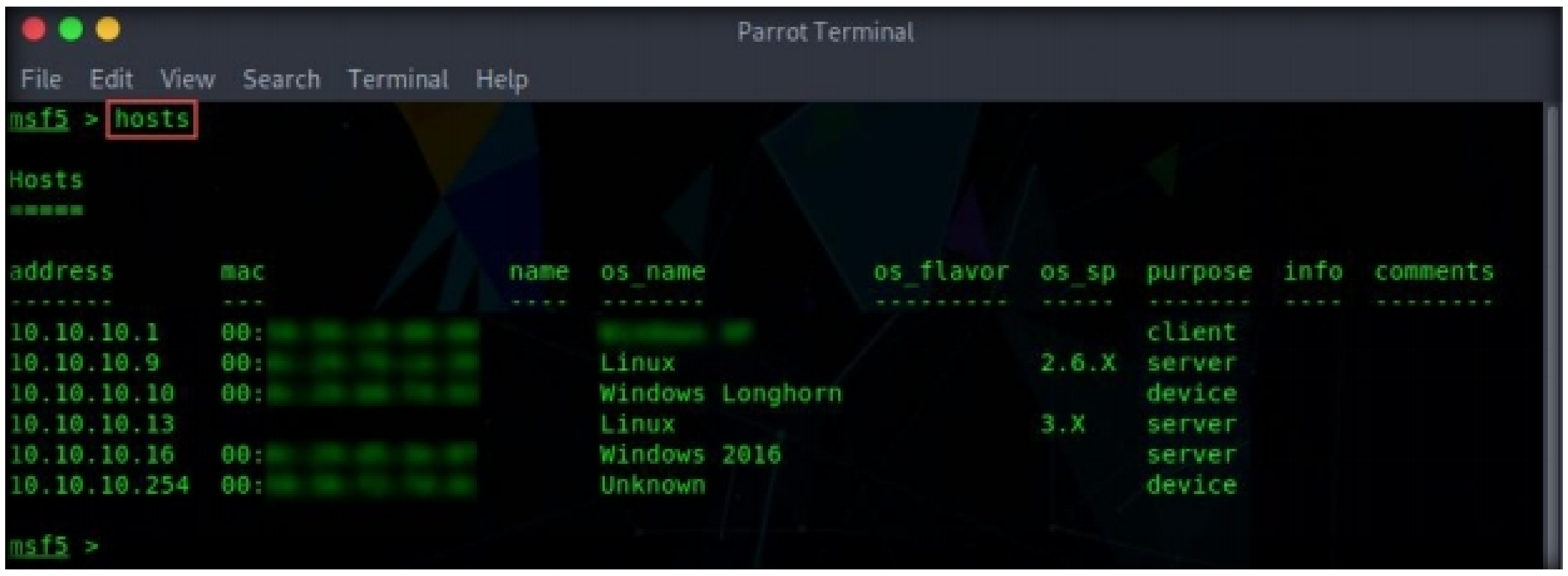
17. Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.



```
msf5 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.2'
[*] Importing host 10.10.10.1
[*] Importing host 10.10.10.9
[*] Importing host 10.10.10.10
[*] Importing host 10.10.10.16
[*] Importing host 10.10.10.254
[*] Importing host 10.10.10.13
[*] Successfully imported /root/Test
msf5 >
```

Figure 6.1.10: Importing Nmap results from the database using Metasploit

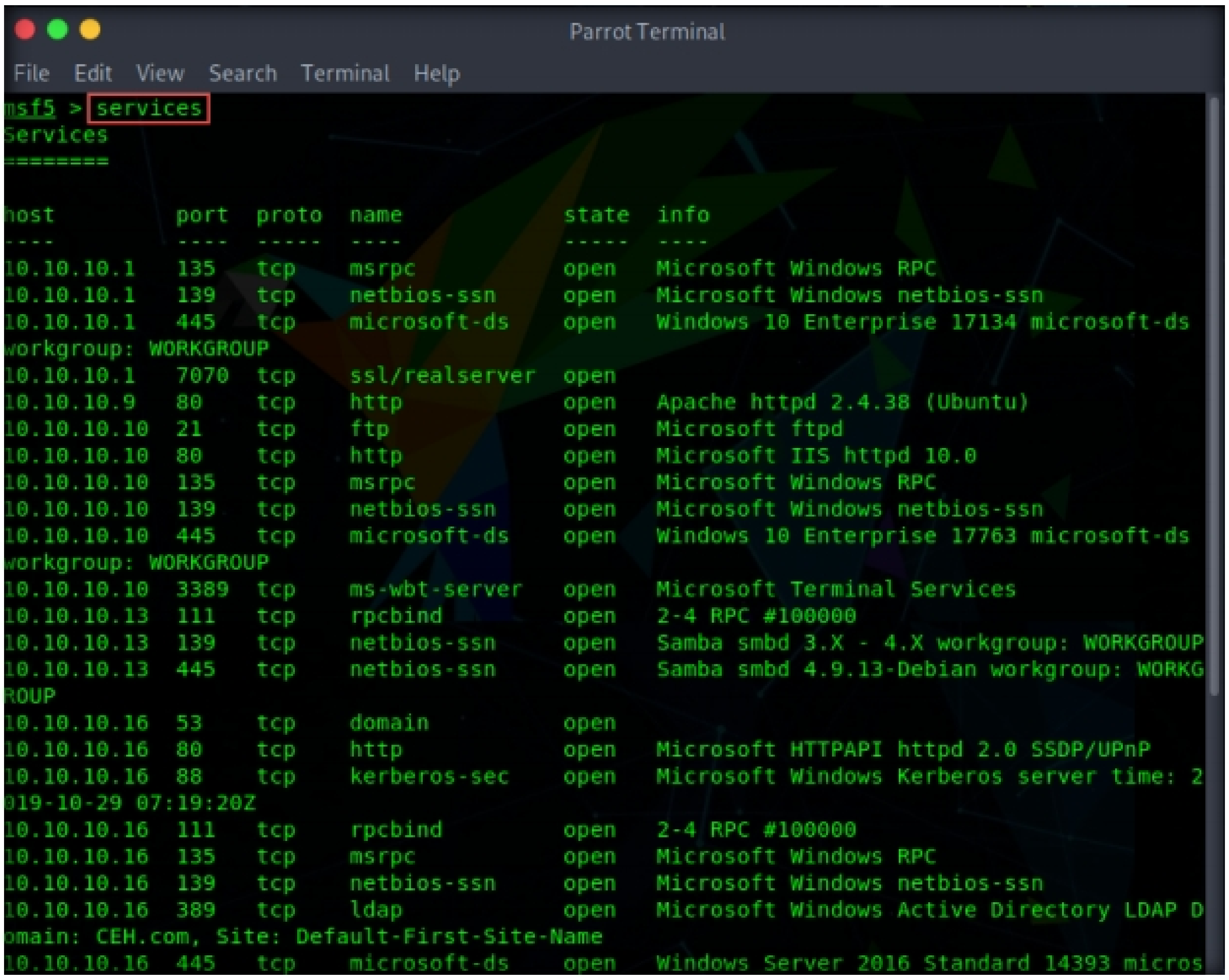
18. Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.



```
msf5 > hosts

Hosts
=====

address       mac                      name  os_name          os_flavor  os_sp  purpose  info  comments
-------       ---                      ----  -------          ---------  -----  -------  ----  --------
10.10.10.1    00:[redacted]                  [redacted]                         client
10.10.10.9    00:[redacted]                  Linux                       2.6.X  server
10.10.10.10   00:[redacted]                  Windows Longhorn                   device
10.10.10.13                                  Linux                       3.X    server
10.10.10.16   00:[redacted]                  Windows 2016                       server
10.10.10.254  00:[redacted]                  Unknown                            device

msf5 >
```

Figure 6.1.11: List of live hosts in the subnet

19. Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.



```
msf5 > services
Services
========

host         port  proto  name            state  info
----         ----  -----  ----            -----  ----
10.10.10.1   135   tcp    msrpc           open   Microsoft Windows RPC
10.10.10.1   139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
10.10.10.1   445   tcp    microsoft-ds    open   Windows 10 Enterprise 17134 microsoft-ds
workgroup: WORKGROUP
10.10.10.1   7070  tcp    ssl/realserver  open
10.10.10.9   80    tcp    http            open   Apache httpd 2.4.38 (Ubuntu)
10.10.10.10  21    tcp    ftp             open   Microsoft ftpd
10.10.10.10  80    tcp    http            open   Microsoft IIS httpd 10.0
10.10.10.10  135   tcp    msrpc           open   Microsoft Windows RPC
10.10.10.10  139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
10.10.10.10  445   tcp    microsoft-ds    open   Windows 10 Enterprise 17763 microsoft-ds
workgroup: WORKGROUP
10.10.10.10  3389  tcp    ms-wbt-server   open   Microsoft Terminal Services
10.10.10.13  111   tcp    rpcbind         open   2-4 RPC #100000
10.10.10.13  139   tcp    netbios-ssn     open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.10.10.13  445   tcp    netbios-ssn     open   Samba smbd 4.9.13-Debian workgroup: WORKG
ROUP
10.10.10.16  53    tcp    domain          open
10.10.10.16  80    tcp    http            open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.16  88    tcp    kerberos-sec    open   Microsoft Windows Kerberos server time: 2
019-10-29 07:19:20Z
10.10.10.16  111   tcp    rpcbind         open   2-4 RPC #100000
10.10.10.16  135   tcp    msrpc           open   Microsoft Windows RPC
10.10.10.16  139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
10.10.10.16  389   tcp    ldap            open   Microsoft Windows Active Directory LDAP D
omain: CEH.com, Site: Default-First-Site-Name
10.10.10.16  445   tcp    microsoft-ds    open   Windows Server 2016 Standard 14393 micros
```

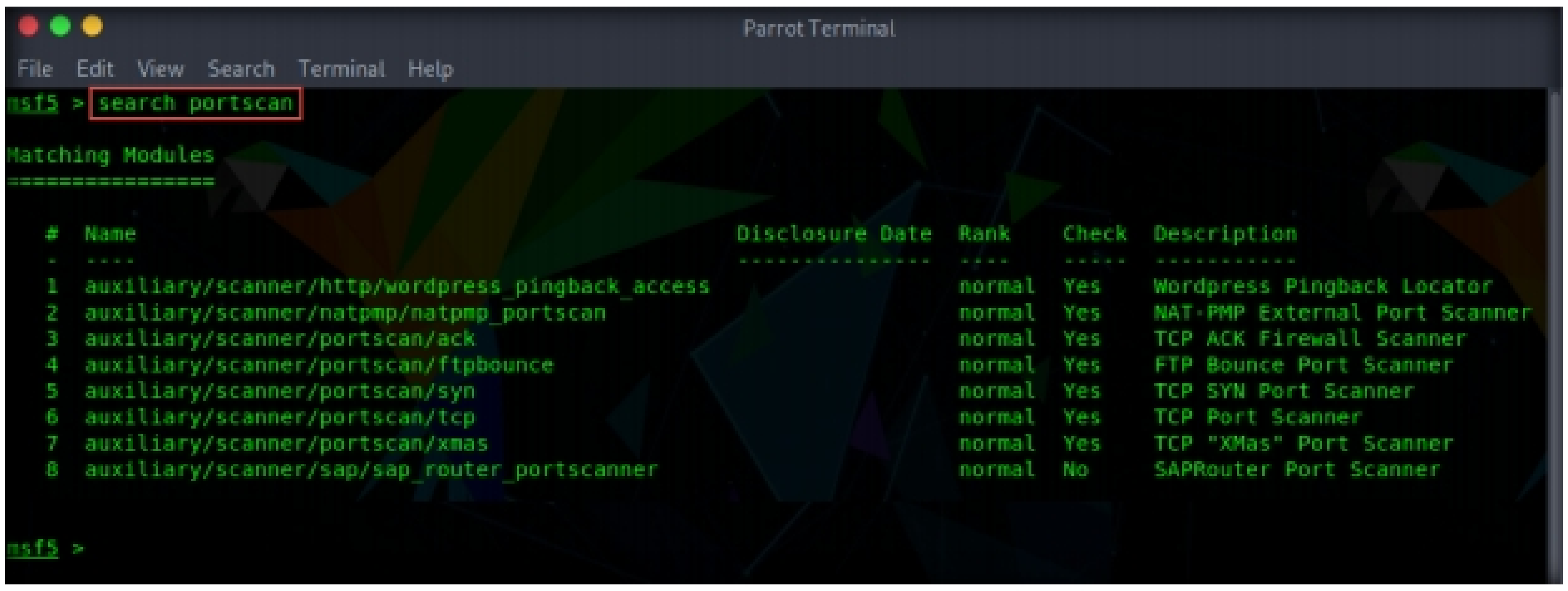
Figure 6.1.12: List of services running on the hosts in the subnet

Note: In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.

TASK 1.3

Perform Port Scanning Using MSF Modules

20. Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.



```
msf5 > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   1  auxiliary/scanner/http/wordpress_pingback_access                   normal  Yes    Wordpress Pingback Locator
   2  auxiliary/scanner/natpmp/natpmp_portscan                           normal  Yes    NAT-PMP External Port Scanner
   3  auxiliary/scanner/portscan/ack                                     normal  Yes    TCP ACK Firewall Scanner
   4  auxiliary/scanner/portscan/ftpbounce                               normal  Yes    FTP Bounce Port Scanner
   5  auxiliary/scanner/portscan/syn                                     normal  Yes    TCP SYN Port Scanner
   6  auxiliary/scanner/portscan/tcp                                     normal  Yes    TCP Port Scanner
   7  auxiliary/scanner/portscan/xmas                                    normal  Yes    TCP "XMas" Port Scanner
   8  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner


msf5 >
```

Figure 6.1.13: List portscan modules

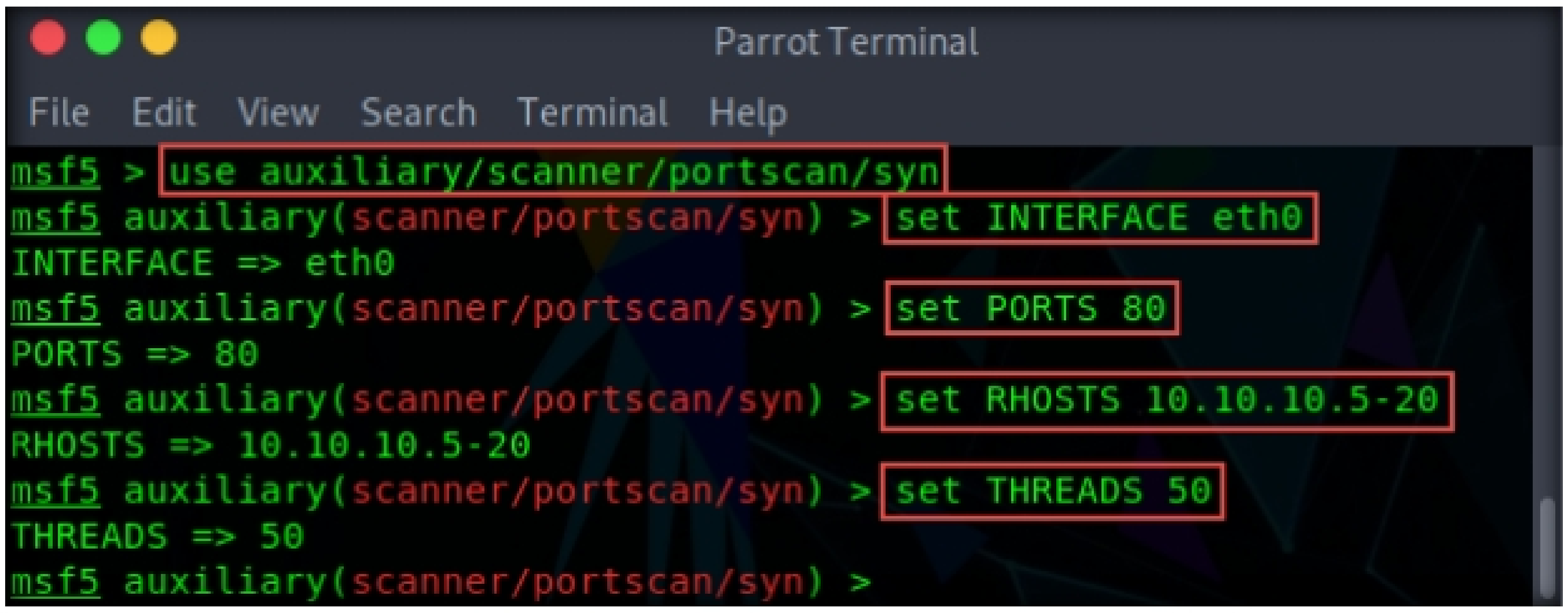
21. Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and press **Enter**.

22. We will use this module to perform an SYN scan against the target IP address range (**10.10.10.5-20**) to look for open port 80 through the eth0 interface.

    To do so, issue the below commands:

    - **set INTERFACE eth0**
    - **set PORTS 80**
    - **set RHOSTS 10.10.10.5-20**
    - **set THREADS 50**

Note: **PORTS**: specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS**: specifies the target address range or CIDR identifier, and **THREADS**: specifies the number of concurrent threads (default 1).



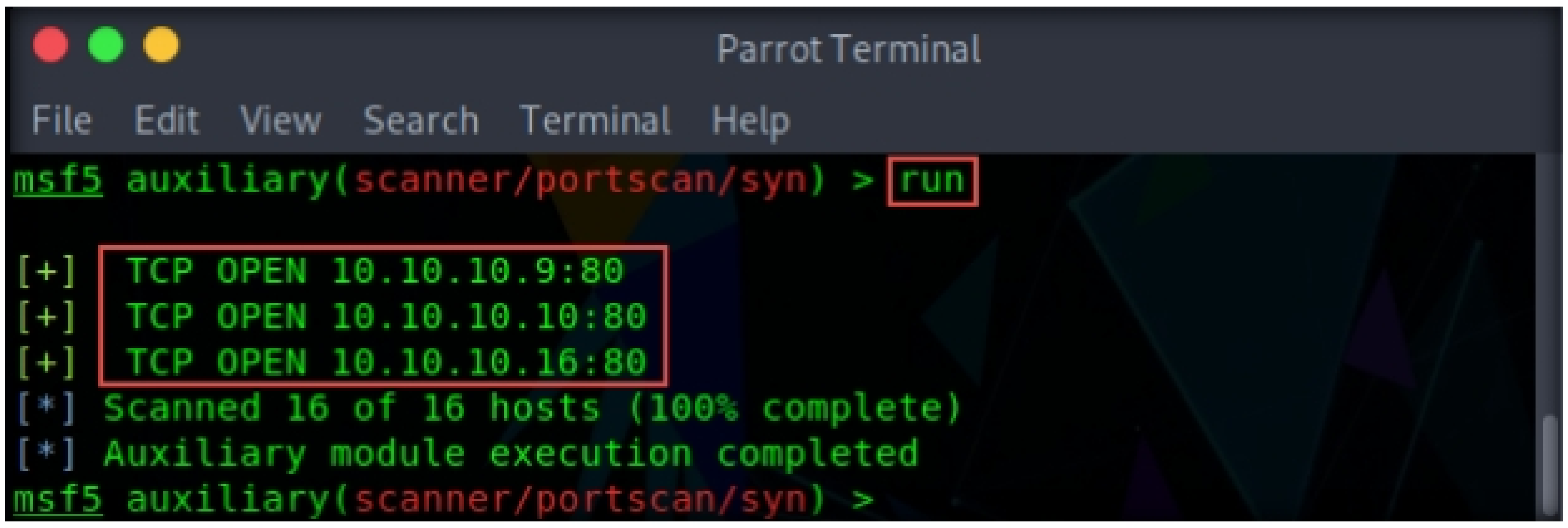
```
msf5 > use auxiliary/scanner/portscan/syn
msf5 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf5 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf5 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf5 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf5 auxiliary(scanner/portscan/syn) >
```

Figure 6.1.14: Setting values to perform a port scan

23. After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

Note: Similarly, you can also specify a range of ports to be scanned against the target IP address range.

24. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.



```
msf5 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 10.10.10.9:80
[+]  TCP OPEN 10.10.10.10:80
[+]  TCP OPEN 10.10.10.16:80
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/syn) >
```

Figure 6.1.15: Port scan result

25. Now, we will perform a TCP scan for open ports on the target systems. To do so, first type **back**, and then press **Enter** to revert to the msf command line.

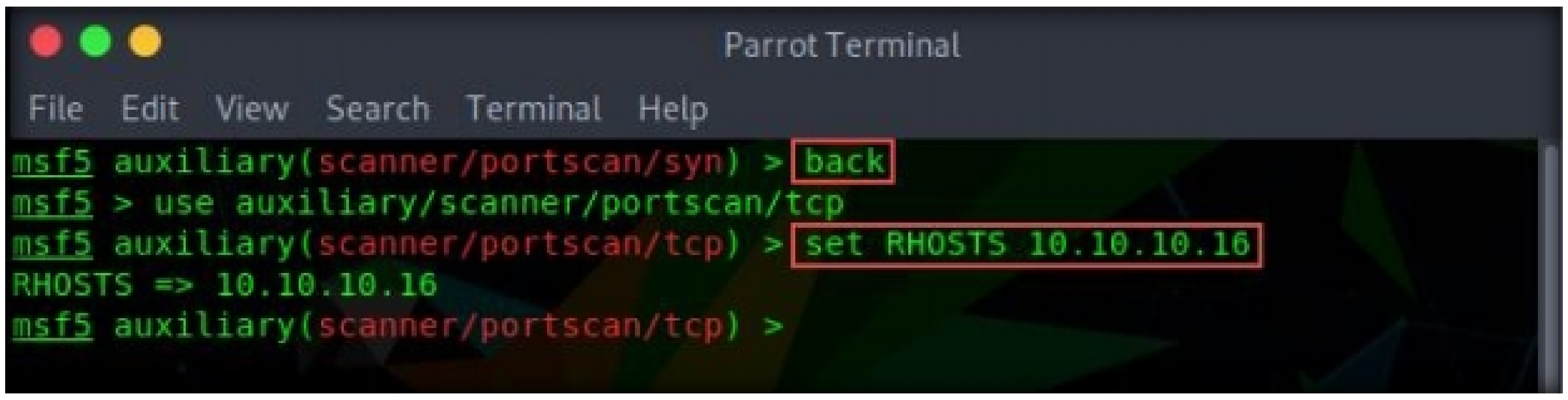
26. To load the auxiliary/scanner/portscan/tcp module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**.

27. Type **hosts -R** and press **Enter** to automatically set this option with the discovered hosts present in our database.

Or

Type **set RHOSTS <Target IP Address>** and press **Enter**.

Note: Here, we will perform a TCP scan for open ports on a single IP address (**10.10.10.16**), as scanning multiple IP addresses consumes much time.

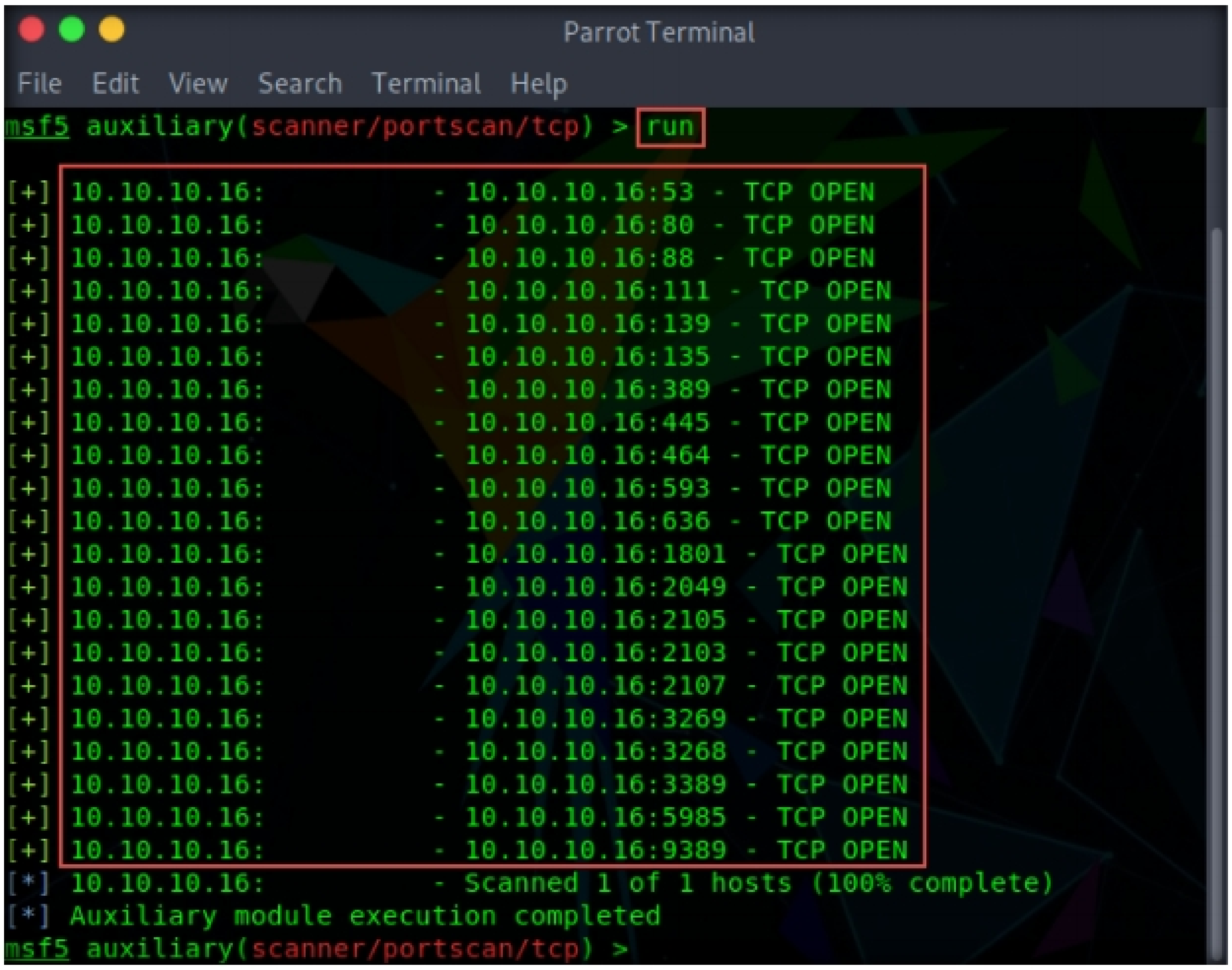


```
msf5 auxiliary(scanner/portscan/syn) > back
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.10.16
RHOSTS => 10.10.10.16
msf5 auxiliary(scanner/portscan/tcp) >
```

Figure 6.1.16: Port scanning using TCP scan

28. Type **run** and press **Enter** to discover open TCP ports in the target system.

29. The results appear, displaying all open TCP ports in the target IP address (10.10.10.16).



```
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.16:          - 10.10.10.16:53 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:80 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:88 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:111 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:139 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:135 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:389 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:445 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:464 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:593 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:636 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:1801 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:2049 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:2105 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:2103 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:2107 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:3269 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:3268 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:3389 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:5985 - TCP OPEN
[+] 10.10.10.16:          - 10.10.10.16:9389 - TCP OPEN
[*] 10.10.10.16:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

Figure 6.1.17: Port scanning using TCP scan

30. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module scanner/smb/version to determine which version of Windows is running on a target and which Samba version is on a Linux host.

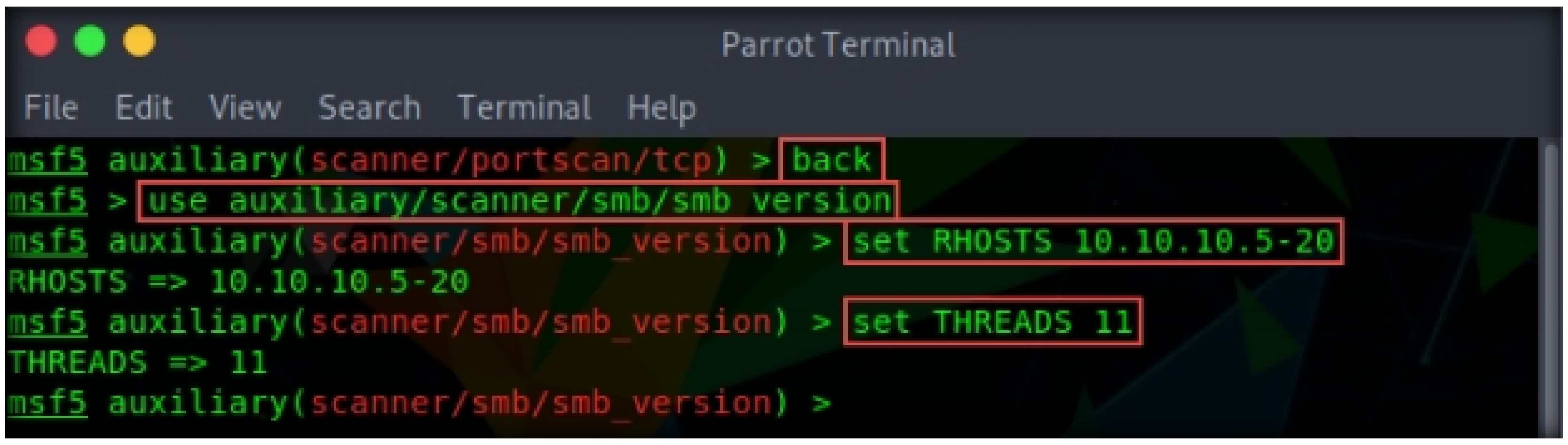
TASK 1.4

SMB Version Scan

31. To do so, first type **back**, and then press **Enter** to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and press **Enter**.

32. We will use this module to run a SMB version scan against the target IP address range (**10.10.10.5-20**). To do so, issue the below commands:

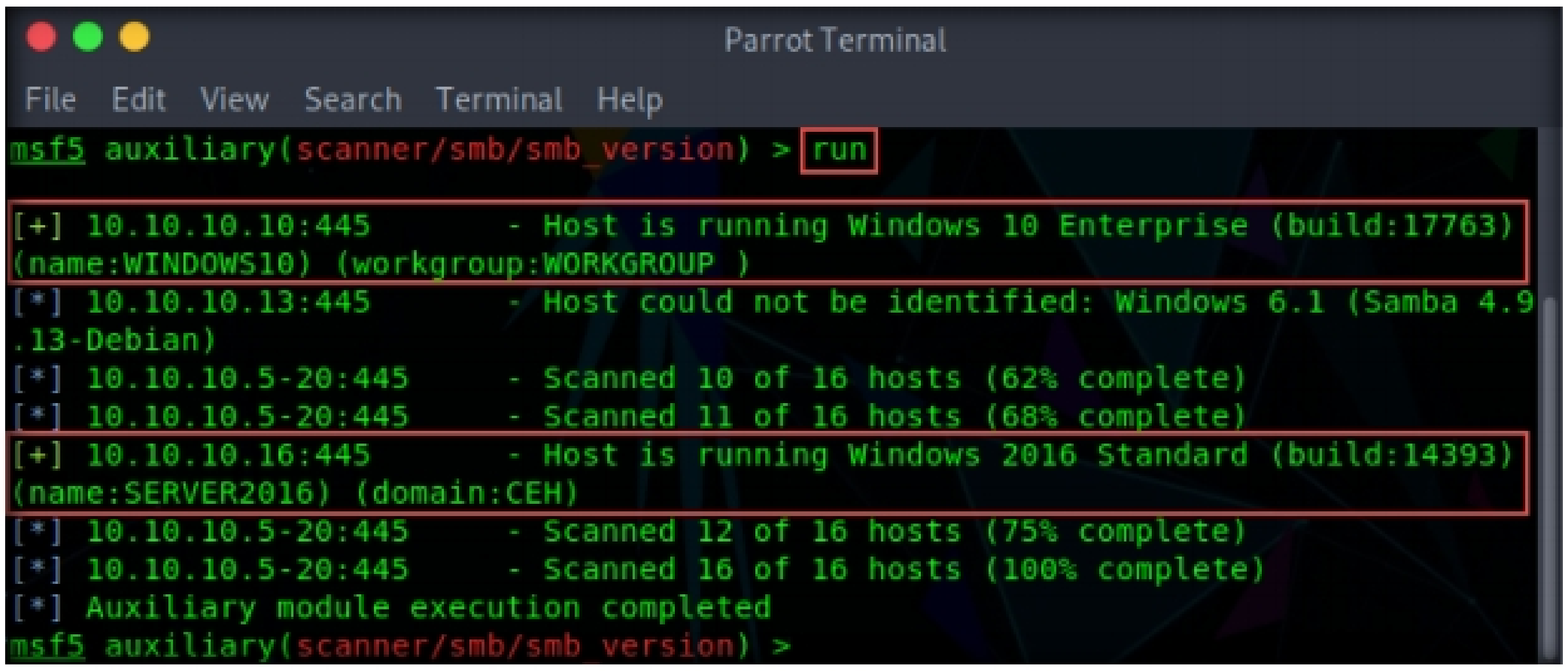
    - **set RHOSTS 10.10.10.5-20**
    - **set THREADS 11**



```
msf5 auxiliary(scanner/portscan/tcp) > back
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf5 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf5 auxiliary(scanner/smb/smb_version) >
```

Figure 6.1.18: SMB version scanning

33. Type **run** and press **Enter** to display the SMB versions of the target hosts.



```
msf5 auxiliary(scanner/smb/smb_version) > run

[+] 10.10.10.10:445       - Host is running Windows 10 Enterprise (build:17763)
(name:WINDOWS10) (workgroup:WORKGROUP )
[*] 10.10.10.13:445       - Host could not be identified: Windows 6.1 (Samba 4.9
.13-Debian)
[*] 10.10.10.5-20:445     - Scanned 10 of 16 hosts (62% complete)
[*] 10.10.10.5-20:445     - Scanned 11 of 16 hosts (68% complete)
[+] 10.10.10.16:445       - Host is running Windows 2016 Standard (build:14393)
(name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20:445     - Scanned 12 of 16 hosts (75% complete)
[*] 10.10.10.5-20:445     - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Figure 6.1.19: SMB version scanning results

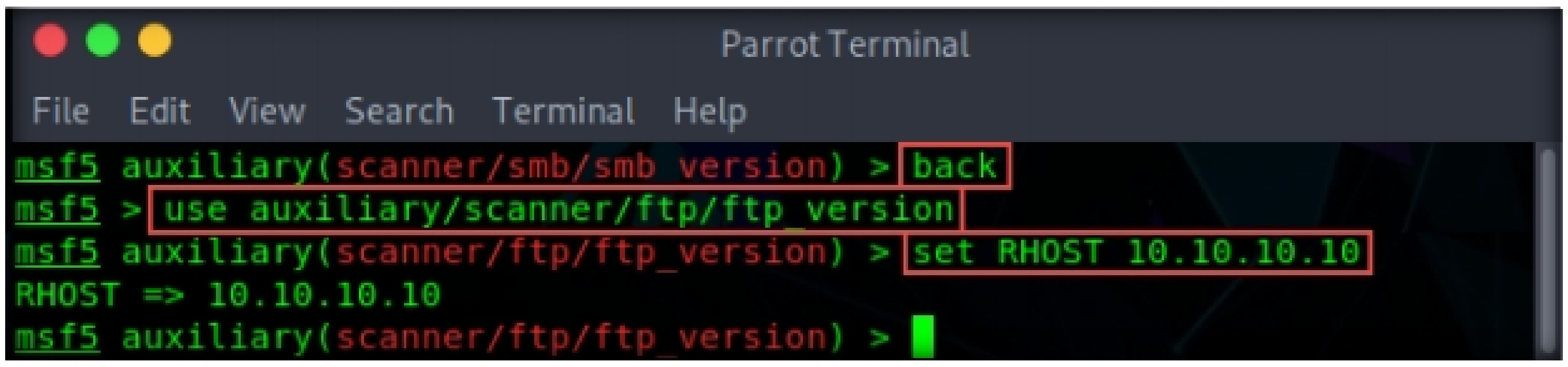
TASK 1.5

FTP Version Identification

34. While performing a scan using Nmap, we discovered that the FTP port 21 is open on the host 10.10.10.10 in the target network. Now, we will scan the target host to identify the FTP version.

35. Type **back** and press **Enter**. To load an FTP module, type **use auxiliary/scanner/ftp/ftp_version** and press **Enter**.

36. Type **set RHOSTS 10.10.10.10** and press **Enter** to specify the target host.

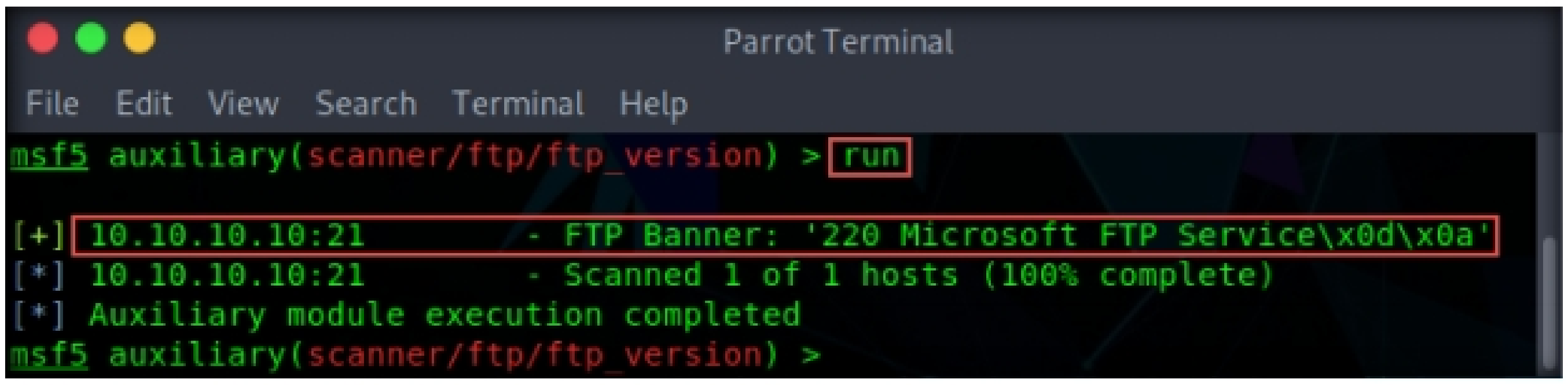


```
msf5 auxiliary(scanner/smb/smb_version) > back
msf5 > use auxiliary/scanner/ftp/ftp_version
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf5 auxiliary(scanner/ftp/ftp_version) > 
```

Figure 6.1.20: FTP version scanning

37. Type **run** and press **Enter** to initiate the FTP version identification scan.

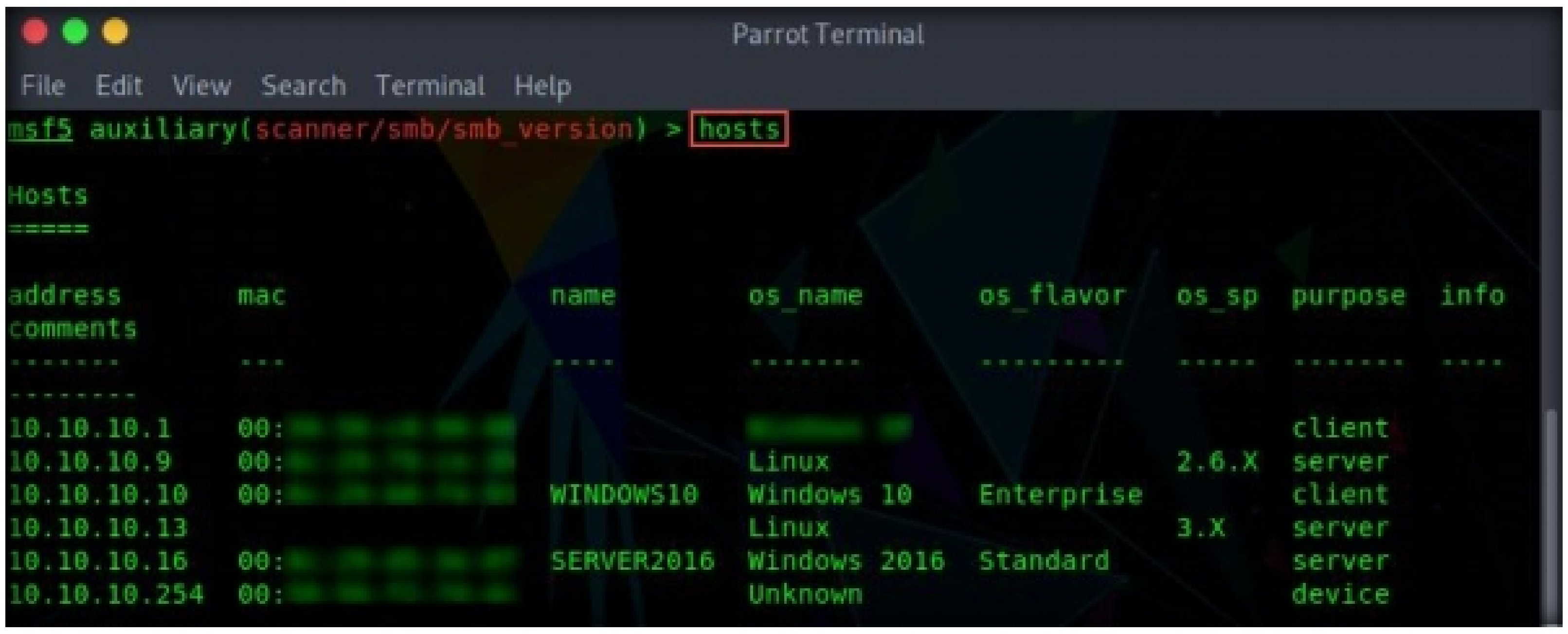
38. The result appears, displaying the FTP version details of the target host, as shown in the screenshot.



```
msf5 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.10.10.10:21         - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 10.10.10.10:21         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_version) >
```

Figure 6.1.21: FTP version identification scan results

39. Type **hosts** and press **Enter** to view detailed information on active hosts in the target network.



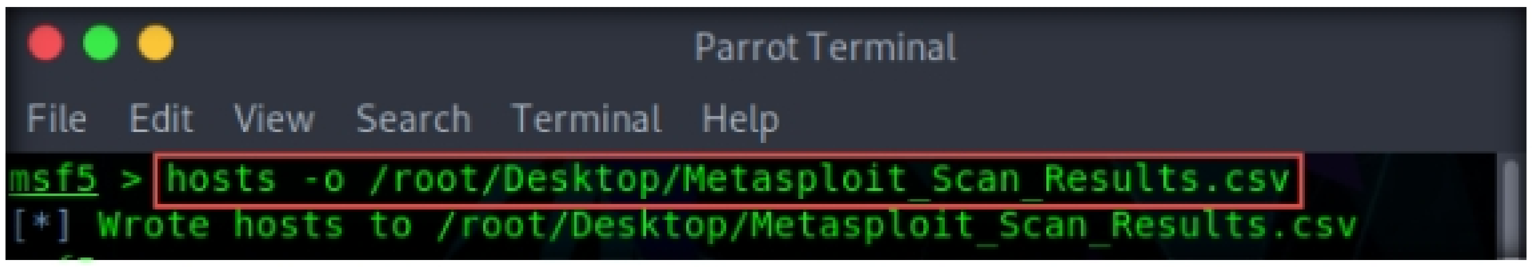
```
msf5 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address       mac                 name        os_name        os_flavor   os_sp  purpose  info
comments
-------       ---                 ----        -------        ---------   -----  -------  ----
--------
10.10.10.1    00:[redacted]                   [redacted]                        client
10.10.10.9    00:[redacted]                   Linux                      2.6.X  server
10.10.10.10   00:[redacted]       WINDOWS10   Windows 10     Enterprise         client
10.10.10.13                                   Linux                      3.X    server
10.10.10.16   00:[redacted]       SERVER2016  Windows 2016   Standard           server
10.10.10.254  00:[redacted]                   Unknown                           device
```

Figure 6.1.22: List of live hosts in the target IP range

TASK 1.6

Export Scan Result

40. You can further export this information to a CSV file. To do so, first type **back**, and then press **Enter**. Now, type **hosts -o /root/Desktop/Metasploit_Scan_Results.csv** and press **Enter**.

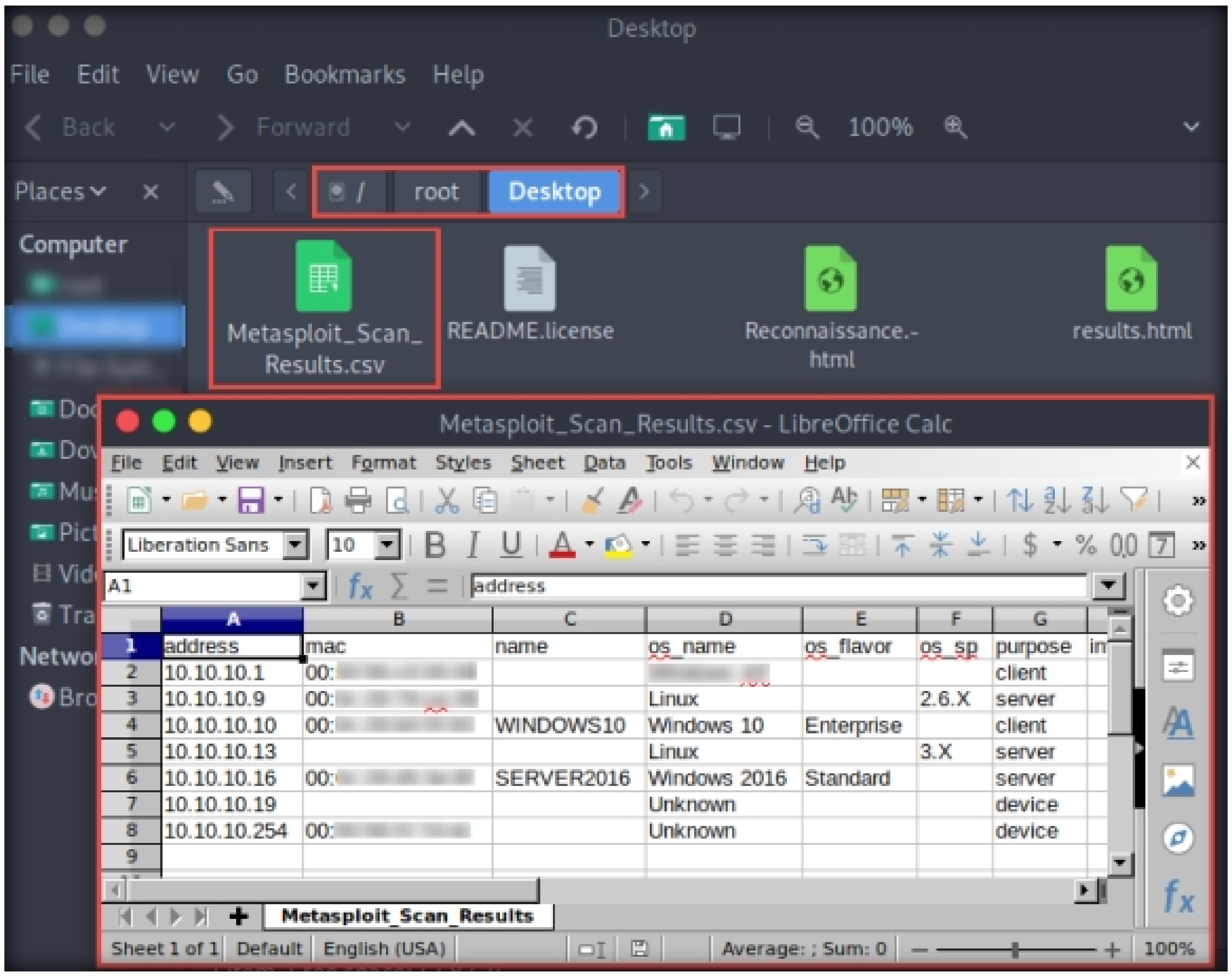


```
msf5 > hosts -o /root/Desktop/Metasploit_Scan_Results.csv
[*] Wrote hosts to /root/Desktop/Metasploit_Scan_Results.csv
```

Figure 6.1.23: Exporting hosts data

41. Navigate to the location **/root/Desktop** and double-click the **Metasploit_Scan_Results.csv** file. The CSV file appears, displaying detailed information on the active hosts in the target IP range.

Note: To navigate to the **Desktop** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root/Desktop**.


Desktop
File Edit View Go Bookmarks Help
Back Forward 100%
Places / root Desktop
Computer
Metasploit_Scan_Results.csv
README.license
Reconnaissance.-html
results.html
Metasploit_Scan_Results.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans 10
A1
Metasploit_Scan_Results
Sheet 1 of 1 Default English (USA) Average: ; Sum: 0 100%

	A	B	C	D	E	F	G	
1	address	mac	name	os_name	os_flavor	os_sp	purpose	in
2	10.10.10.1	00:[redacted]		[redacted]			client	
3	10.10.10.9	00:[redacted]		Linux		2.6.X	server	
4	10.10.10.10	00:[redacted]	WINDOWS10	Windows 10	Enterprise		client	
5	10.10.10.13			Linux		3.X	server	
6	10.10.10.16	00:[redacted]	SERVER2016	Windows 2016	Standard		server	
7	10.10.10.19			Unknown			device	
8	10.10.10.254	00:[redacted]		Unknown			device	
9								

Figure 6.1.24: Exported hosts information

42. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.

43. This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.

44. Close all open windows and document all the acquired information.

45. Turn off the **Windows 10**, **Windows Server 2016**, **Ubuntu**, and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs